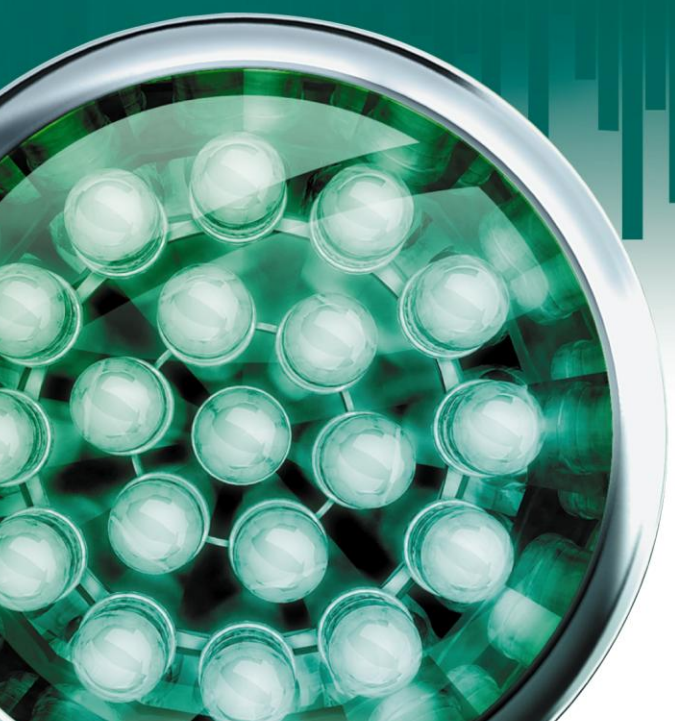
Kaspersky Anti-Virus 6.0 für Windows Server MP4

BENUTZERHANDBUCH

PROGRAMMVERSION: 6.0 MAINTENANCE PACK 4 CRITICAL FIX 1



KASPERSKY lab

Sehr geehrter Benutzer!

Vielen Dank, dass Sie unser Produkt ausgewählt haben. Wir hoffen, dass diese Dokumentation Ihnen hilft und die meisten Fragen damit beantwortet werden können.

Redaktionsdatum: 03.02.2010

http://www.kaspersky.de
http://support.kaspersky.de

INHALT

EINLEITUNG

IN DIESEM ABSCHNITT

LIEFERUMFANG

Kaspersky Internet Security kann bei unseren Vertriebspartnern (als verpackte Variante) oder in einem Online-Shop (z.B. http://www.kaspersky.com/de, Abschnitt **E-Store**) erworben werden.

Wurde das Programm in einer CD-Box erworben, gehören zum Lieferumfang des Programms:

- Versiegelter Umschlag mit Installations-CD, auf der die Programmdateien und die Dokumentation im PDF-Format gespeichert sind.
- Benutzerhandbuch in gedruckter Form (wenn diese Position im Auftrag enthalten war) oder Benutzerhandbuch.
- Schlüsseldatei für die Anwendung (auf einer speziellen Diskette gespeichert).
- Lizenzvertrag

Bevor Sie den Umschlag mit der CD (oder den Disketten) aufbrechen, lesen Sie sich bitte die Lizenzvereinbarung sorgfältig durch.

Beim Erwerb von Kaspersky Anti-Virus in einem Online-Shop kopieren Sie das Produkt von der Kaspersky-Lab-Internetseite. Die Distribution enthält neben dem eigentlichen Produkt auch die vorliegende Dokumentation. Eine Schlüsseldatei wird Ihnen nach Eingang der Bezahlung per E-Mail zugeschickt.

LIZENZVERTRAG

Die Lizenzvereinbarung ist ein juristischer Vertrag zwischen Ihnen und Kaspersky Lab ZAO, in dem steht, unter welchen Bedingungen Sie das von Ihnen gekaufte Programm gebrauchen dürfen.

Lesen Sie sich die Lizenzvereinbarung genau durch!

Wenn Sie die Bedingungen der Lizenzvereinbarung nicht annehmen, können Sie die Box an den Fachhändler zurückgeben, bei dem Sie sie gekauft haben, und Sie bekommen Ihr Geld zurück. Der Umschlag mit der Installations-CD (oder Disketten) muss noch versiegelt sein.

Wenn Sie den versiegelten Umschlag mit der Installations-CD (oder den Disketten) öffnen, nehmen Sie dadurch alle Bedingungen in der Lizenzvereinbarung an.

SERVICE FÜR REGISTRIERTE BENUTZER

Kaspersky Lab bietet legalen Benutzern ein breites Spektrum an Serviceleistungen, die eine gesteigerte Effektivität von Kaspersky Anti-Virus ermöglichen.

Wenn Sie eine Lizenz erwerben, werden Sie ein registrierter Benutzer und während der Gültigkeitsdauer der Lizenz können Sie folgende Leistungen in Anspruch nehmen:

- stündliches Update der Programm-Datenbanken und Nutzung neuer Versionen des betreffenden Softwareprodukts.
- Beratung bei Fragen zur Installation, Konfiguration und Nutzung des Programms per Telefon und E-Mail;
- Benachrichtigung bei Herausgabe von neuen Kaspersky-Lab-Programmen und bei neu aufgetauchten Viren. Dieser Service wird Benutzern geboten, die den Newsletter von Kaspersky Lab auf der Webseite des Technischen Supports (http://support.kaspersky.de/subscribe/) abonniert haben.

Es werden allerdings keine Fragen zu Funktion und Gebrauch von Betriebssystemen, zu Programmen von Dritten sowie zu verschiedenen Technologien beantwortet.

HARD- UND SOFTWAREVORAUSSETZUNGEN FÜR DAS SYSTEM

Um die normale Funktionsfähigkeit von Kaspersky Anti-Virus 6.0 zu gewährleisten, muss der Computer mindestens folgende Voraussetzungen erfüllen:

Allgemeine Anforderungen:

- 300 MB freier Speicher auf der Festplatte.
- Microsoft Internet Explorer 6.0 oder höher (für das Update der Datenbanken und Programm-Module über das Internet).
- Microsoft Windows Installer 2.0 oder höher.

Windows 2000 Server / Advanced Server (Service Pack 4 Rollup1), Windows Server 2003 Standard / Enterprise (Service Pack 2), Windows Server 2003 x64 Standard / Enterprise (Service Pack 2), Windows Small Business Server 2003:

- Prozessor Intel Pentium 400 MHz 32-Bit (x86) / 64-Bit (x64) oder höher (oder ein entsprechender kompatibler Prozessor).
- 512 MB Arbeitsspeicher.

Windows Server 2003 R2 Standard / Enterprise Edition, Windows Server 2003 R2 x64 Standard / Enterprise Edition, Windows Server 2008 Standard / Enterprise (Service Pack 1 oder höher), Windows Server 2008 x64 Standard / Enterprise (Service Pack 1 oder höher), Windows Small Business Server 2008, Windows Essential Business Server 2008, Windows Server 2008 R2 x64 Standard / Enterprise:

- Prozessor Intel Pentium 1 ННц 32-bit (x86) / 1,4 ННц 64-bit (x64) oder höher (oder ein entsprechender kompatibler Prozessor).
- 1 GB Arbeitsspeicher.

KASPERSKY ANTI-VIRUS 6.0 FÜR WINDOWS SERVER MP4

Kaspersky Anti-Virus 6.0 für Windows Server MP4 ist eine neue Generation des Informationsschutzes.

In diesem Abschnitt

Suche nach Informationen über das Programm

Wenn Sie Fragen zu Auswahl, Kauf, Installation oder Verwendung von Kaspersky Anti-Virus haben, können Sie schnell eine Antwort darauf erhalten.

Kaspersky Lab bietet unterschiedliche Informationsquellen zu dem Programm an. Sie können abhängig von der Dringlichkeit und Bedeutung Ihrer Frage unter diesen Quellen wählen.

In diesem Abschnitt

Informationsquellen zur selbständigen Recherche

Bei Fragen über die Anwendung stehen folgende Informationsquellen zur Verfügung:

- Seite über das Programm auf der Webseite von Kaspersky Lab.
- Seite über das Programm auf der Webseite des Technischen Supports (in der Wissensdatenbank).
- elektronisches Hilfesystem
- Dokumentationen.

Seite über das Produkt auf der Webseite von Kaspersky Lab

http://www.kaspersky.com/de/anti-virus_windows_server

Auf dieser Seite finden Sie allgemeine Informationen über das Programm, seine Funktionen und Besonderheiten.

Seite auf der Webseite des Technischen Supports (Wissensdatenbank)

http://support.kaspersky.com/de/windows_file_server

Auf dieser Seite finden Sie Artikel, die von Spezialisten des Technischen Supports veröffentlicht wurden.

Diese Artikel bieten nützliche Informationen, Tipps und Antworten auf häufige Fragen zu Kauf, Installation und Verwendung vom Programm. Sie sind nach Themen wie "Arbeit mit Schlüsseldateien", "Konfiguration des Datenbank-Updates" oder "Beheben von Störungen bei der Arbeit" angeordnet. Die Artikel können auch Fragen behandeln, die neben diesem Programm auch andere Produkte von Kaspersky Lab betreffen. Außerdem können sie allgemeine Neuigkeiten über den Technischen Support enthalten.

Elektronisches Hilfesystem

Im Lieferumfang des Programms ist eine vollständige und kontextorientierte Hilfedatei enthalten. Sie bietet Informationen zu folgenden Aspekten der Verwaltung des Computerschutzes: Anzeige des Schutzstatus, Untersuchung bestimmter Computerbereiche auf Viren, Ausführen anderer Aufgaben, sowie Informationen zu jedem Fenster der Anwendung: Liste und Beschreibung der in einem Fenster vorhandenen Parameter und Liste der ausführbaren Aufgaben.

Um die Hilfe zu öffnen, klicken Sie im entsprechenden Fenster auf die Schaltfläche **Hilfe** oder auf die Taste **<F1>**.

Dokumentation

Zum Lieferumfang von Kaspersky Anti-Virus gehört das Dokument **Benutzerhandbuch** (im PDF-Format). Dieses Dokument enthält eine Beschreibung der Funktionen und Möglichkeiten der Anwendung und beschreibt die wichtigsten Funktionsalgorithmen.

KONTAKTAUFNAHME MIT DER VERTRIEBSABTEILUNG

Bei Fragen zur Auswahl oder zum Kauf von Kaspersky Anti-Virus sowie zur Verlängerung der Nutzungsdauer stehen Ihnen die Mitarbeiter der Vertriebsabteilung in unserer Zentrale in Moskau unter folgenden Telefonnummern zur Verfügung:

+7 (495) 797-87-00 , **+7 (495) 645-79-39**, **+7 (495) 956-70-00**

Die Beratung kann auf Englisch oder Russisch erfolgen.

Sie können sich mit Ihrer Frage auch unter folgender Adresse per E-Mail an die Mitarbeiter der Vertriebsabteilung wenden: sales@kaspersky.com.

KONTAKTAUFNAHME MIT DEM TECHNISCHEN SUPPORT

Wenn Sie die Kaspersky Anti-Virus bereits erworben haben, können Sie von den Spezialisten des Technischen Supports per Telefon oder über das Internet Informationen darüber erhalten.

Die Support-Spezialisten beantworten Ihre Fragen, die die Installation und Verwendung des Programms betreffen und nicht in der Hilfe beschrieben werden, und helfen Ihnen dabei, die Folgen von Virenangriffen zu beheben, wenn Ihr Computer infiziert wurde.

Bevor Sie sich an den Technischen Support wenden, lesen Sie sich bitte zuvor die Supportrichtlinien (http://support.kaspersky.com/de/support/rules) durch.

E-Mail-Anfrage an den Technischen Support

Sie können Ihre Frage den Spezialisten des Technischen Supports stellen. Füllen Sie dazu das Webformular im System für Kundenanfragen Helpdesk aus (http://support.kaspersky.ru/helpdesk.html?LANG=de).

Die Anfrage kann in deutscher, englischer, französischer, spanischer oder russischer Sprache gestellt werden.

Um eine E-Mail-Anfrage zu stellen, ist die Angabe der **Kundennummer**, die Sie bei der Anmeldung auf der Webseite des Technischen Supports erhalten haben, und des **Kennworts** erforderlich.

Wenn Sie noch nicht als Benutzer eines Kaspersky-Lab-Programms registriert sind, können Sie ein Anmeldeformular (https://support.kaspersky.com/ru/personalcabinet/Registration/Form/?LANG=de) ausfüllen. Geben Sie bei der Anmeldung den *Aktivierungscode* des Programms oder den *Namen der Schlüsseldatei* an.

Die Support-Spezialisten werden Ihre Frage in Ihrem Personal Cabinet Personal Cabinet (https://support.kaspersky.com/de/PersonalCabinet) und per E-Mail an die in der Anfrage angegebene Adresse beantworten.

Beschreiben Sie im Webformular das aufgetretene Problem möglichst genau. Machen Sie in den obligatorisch auszufüllenden Feldern folgende Angaben:

- **Typ der Anfrage**. Wählen Sie das Thema aus, zu dem Ihr Problem gehört (z.B. "Problem bei der Installation/Deinstallation des Produkts" oder "Problem bei der Suche/Desinfektion von Viren". Wenn keine der Kategorien zutrifft, wählen Sie den Punkt "Allgemeine Frage".
- **Name und Versionsnummer des Programms**.
- **Anfragetext**. Beschreiben Sie das Problem möglichst genau.
- **Kundennummer und Kennwort**. Geben Sie die Kundennummer und das Kennwort an, die Sie bei der Anmeldung auf der Support-Webseite erhalten haben.
- **E-Mail-Adresse**. An diese Adresse werden die Support-Spezialisten Ihre Anfrage beantworten.

Technischer Support am Telefon

Zur Lösung dringender Probleme können Sie Ihren lokalen Technischen Support anrufen. Wenn Sie sich an den russischsprachigen (http://support.kaspersky.ru/support/support_local) oder internationalen (http://support.kaspersky.com/de/support/international) Technischen Support wenden, um Hilfe zu erhalten, vergessen Sie bitte nicht, die dafür erforderlichen Informationen (http://support.kaspersky.com/de/support/details) über Ihren Computer und das installierte Antiviren-Programm bereitzuhalten. Dadurch können unsere Spezialisten Ihnen möglichst schnell helfen.

DISKUSSION ÜBER DIE PROGRAMME VON KASPERSKY LAB IM WEBFORUM

Wenn Ihre Frage keine dringende Antwort erfordert, können Sie sie mit den Spezialisten von Kaspersky Lab und mit anderen Anwendern in unserem Forum unter der Adresse http://forum.kaspersky.com diskutieren.

Im Forum können Sie bereits veröffentlichte Themen nachlesen, eigene Beiträge schreiben, neue Themen eröffnen und die Hilfefunktion verwenden.

NEUERUNGEN IN KASPERSKY ANTI-VIRUS 6.0 FÜR WINDOWS SERVER MP4

Kaspersky Anti-Virus 6.0 ist ein universelles Programm für den Informationsschutz. Im Folgenden werden die Neuerungen in Kaspersky Anti-Virus 6.0 ausführlich beschrieben.

Neuerungen im Schutz:

- Der neue Antiviren-Kern, auf dem Kaspersky Anti-Virus basiert, erhöht die Effektivität der Suche nach schädlichen Programmen. Außerdem wird durch den neuen Antiviren-Kern die Geschwindigkeit für die Virenuntersuchung des Systems wesentlich gesteigert. Dies wird erreicht durch eine verbesserte Objektverarbeitung und eine optimierte Nutzung der Computerressourcen (speziell bei Plattformen mit Zwei- und Vierkernprozessoren).

- Neuer heuristischer Analysator, der eine erhöhte Effektivität bei der Erkennung und Sperrung bisher unbekannter Malware bietet. Wenn die Signatur eines Programms nicht in den Antiviren-Datenbanken enthalten ist, emuliert der heuristische Analysator den Start des Programms in einer isolierten virtuellen Umgebung. Diese Methode ist ungefährlich und erlaubt es, alle Funktionen eines Programms zu analysieren, bevor es unter realen Bedingungen gestartet wird.

- Der Vorgang für das Programm-Update wurde optimiert: Ein Neustart des Computers ist jetzt nur noch in seltenen Fällen erforderlich.

Neuerungen auf der Programmoberfläche:

- Das Interface bietet einfachen und komfortablen Zugriff auf alle Programmkomponenten.

- Das Interface ist für die Administratoren kleiner Netzwerke und großer Firmennetzwerke ausgelegt.

Neuerungen bei der Arbeit mit Kaspersky Administration Kit:

- Kaspersky Administration Kit dient der bequemen und einfachen Verwaltung des Schutzsystems eines Unternehmens. Die Anwendung ermöglicht die zentrale Steuerung des Schutzsystems von Firmennetzwerken jeder Größe mit bis zu zehntausend Clients, einschließlich externer und mobiler Anwender.

- Eine Möglichkeit zur Remote-Installation der Anwendung mit der letzten Version der Programm-Datenbanken wurde realisiert.

- Der Mechanismus, der für die Arbeit mit der Anwendung eingesetzt wird, wenn diese auf einem Remote-Computer installiert ist, wurde optimiert (Die Richtlinienstruktur wurde überarbeitet).

- Beim Erstellen einer Richtlinie kann jetzt die Konfigurationsdatei der Anwendung verwendet werden.

- In den Parametern gruppenbezogener Updateaufgaben können jetzt spezifische Parameter für mobile Benutzer festgelegt werden.

- Es ist jetzt möglich, Client-Computer, auf denen die Anwendung installiert ist, vorübergehend aus dem Gültigkeitsbereich von Richtlinien und Gruppenaufgaben zu entnehmen (nach Eingabe des festgelegten Kennworts).

SCHUTZPRINZIPIEN VON KASPERSKY ANTI-VIRUS

Der Schutz umfasst:

- Datei-Anti-Virus (auf S. 14), der die Objekte des Dateisystems eines Computers in Echtzeit überwacht.

- Untersuchungsaufgaben (auf S. 15), mit denen der gesamte Computer oder einzelne Dateien, Ordner, Laufwerke oder Bereiche auf Viren untersucht werden kann.

- Update (auf S. 15), das den aktuellen Zustand der internen Programm-Module sowie der Datenbanken, die der Suche nach schädlichen Programmen dienen, gewährleistet.

- Servicefunktionen (s. Abschnitt "Servicefunktionen des Programms" auf S. 15), die Informationen über die Arbeit mit dem Programm bieten und es erlauben, die Programmfunktionalität zu erweitern.

DATEI-ANTI-VIRUS

Der Schutz des Servers wird mit Hilfe von Datei-Anti-Virus gewährleistet.

Das Dateisystem kann Viren und andere gefährliche Programme enthalten. Nachdem Schädlinge über einen Wechseldatenträger oder das Internet eingedrungen sind, können sie sich jahrelang im Dateisystem eines Computers befinden, ohne dass ihre Existenz bemerkt wird. Sobald eine infizierte Datei aber geöffnet wird, kann der Virus aktiv werden.

Datei-Anti-Virus – ist eine Komponente, die das Dateisystem des Computers kontrolliert. Er untersucht auf dem Computer und auf allen angeschlossenen Laufwerken alle Dateien, die geöffnet, gestartet und gespeichert werden. Jeder Zugriff auf eine Datei wird von Kaspersky Anti-Virus abgefangen und die Datei wird auf die Existenz bekannter Viren untersucht. Eine Datei wird nur dann zur Arbeit freigegeben, wenn die Datei virenfrei ist oder erfolgreich vom Programm desinfiziert wurde. Wenn die Desinfektion der Datei aus bestimmten Gründen nicht möglich ist, wird sie gelöscht, dabei wird eine Kopie der Datei im Backup abgelegt oder in die Quarantäne verschoben.

AUFGABEN ZUR VIRENSUCHE

Neben dem Schutz, den Datei-Anti-Virus bietet, ist es sehr wichtig, den Server regelmäßig vollständig auf Viren zu untersuchen. Das ist erforderlich, um die Ausbreitung schädlicher Programme auszuschließen, die nicht von Datei-Anti-Virus erkannt wurden, weil beispielsweise eine zu geringe Schutzstufe eingestellt war.

Kaspersky Anti-Virus verfügt über folgende Aufgaben zur Virensuche:

Virensuche

Untersuchung von Objekten, die der Benutzer festlegt. Sie können ein beliebiges Objekt des Dateisystems auf dem Computer untersuchen.

Vollständige Suche

Ausführliche Untersuchung des Systems. Standardmäßig werden folgende Objekte untersucht: Systemspeicher, Objekte, die beim Systemstart gestartet werden, Systemwiederherstellung, Mail-Datenbanken, Festplatten, Wechseldatenträger und Netzlaufwerke.

Schnelle Suche

Virenuntersuchung der Objekte, die beim Start des Betriebssystems geladen werden.

UPDATE

Um stets bereit zu sein, Hackerangriffe abzuwehren und Viren oder andere gefährliche Programme zu neutralisieren, ist es erforderlich, den aktuellen Zustand von Kaspersky Anti-Virus zu gewährleisten. Dazu dient die Komponente **Update**. Sie ist für die Aktualisierung der Datenbanken und Programm-Module verantwortlich, die bei der Arbeit des Programms verwendet werden.

Der Dienst zur Update-Verteilung erlaubt es, die Updates für Datenbanken und Programm-Module, die von den Kaspersky-Lab-Updateservern heruntergeladen wurden, in einem lokalen Ordner zu speichern. Dieser Ordner kann anderen Netzwerkcomputern als Updatequelle dienen, um Datenverkehr einzusparen.

SERVICEFUNKTIONEN DES PROGRAMMS

Kaspersky Anti-Virus verfügt über eine Reihe von Servicefunktionen. Sie dienen dazu, den aktuellen Zustand des Programms aufrechtzuerhalten, die Optionen des Programms zu erweitern und bei der Arbeit Hilfe zu leisten.

Datenverwaltung

Bei der Arbeit der Anwendung wird für jede Schutzkomponente, Untersuchungsaufgabe und Updateaufgabe der Anwendung ein Bericht erstellt. Er enthält Informationen über die ausgeführten Operationen und die Arbeitsergebnisse. Dadurch können Sie jederzeit Details über die Arbeit einer beliebigen Aufgabe nachlesen. Sollten Probleme auftreten, dann können Sie die Berichte an Kaspersky Lab schicken, damit unsere Experten die Situation analysieren und Ihnen möglichst schnell helfen können.

Alle im Hinblick auf die Sicherheit verdächtigen Objekte werden von Kaspersky Anti-Virus in den speziellen Speicher *Quarantäne* verschoben. Sie werden dort in verschlüsselter Form gespeichert, um eine Infektion des Computers auszuschließen. Sie können die Quarantäneobjekte auf Viren untersuchen, am ursprünglichen Ort wiederherstellen oder löschen. Außerdem können Sie verdächtige Objekte manuell in die Quarantäne verschieben. Alle Objekte, die sich aufgrund der Untersuchung als virenfrei erweisen, werden automatisch am ursprünglichen Ort wiederhergestellt.

Im *Backup* werden Kopien von Objekten gespeichert, die von der Anwendung desinfiziert und gelöscht wurden. Diese Kopien werden angelegt, um bei Bedarf die Objekte oder ein Bild der Infektion wiederherzustellen. Auch die Sicherungskopien der Objekte werden in verschlüsselter Form gespeichert, um eine Infektion des Computers auszuschließen.

Sie können ein Objekt aus dem Backup am ursprünglichen Ort wiederherstellen oder die Sicherungskopie löschen.

Rettungs-Disk

Die Rettungs-Disk dient zur Untersuchung und Desinfektion infizierter x86-kompatibler Computer. Sie kommt dann zum Einsatz, wenn der Infektionsgrad so hoch ist, dass die Desinfektion eines Computers nicht mehr mit Hilfe von Antiviren-Anwendungen oder Desinfektionstools möglich ist.

Lizenz

Beim Kauf von Kaspersky Anti-Virus wird zwischen Ihnen und Kaspersky Lab ein Lizenzvertrag abgeschlossen, auf dessen Grundlage Sie die Anwendung verwenden dürfen und für einen festgelegten Zeitraum Zugriff auf Updates für die Programm-Datenbanken und auf den Technischen Support erhalten. Die Nutzungsdauer sowie andere Informationen, die für die vollfunktionale Arbeit der Anwendung erforderlich sind, sind in der Lizenz angegeben.

Mit der Funktion **Lizenz** können Sie ausführliche Informationen über die von Ihnen verwendete Lizenz erhalten. Außerdem können Sie damit eine neue Lizenz erwerben oder die Gültigkeit der aktiven Lizenz verlängern.

Support

Alle registrierten Benutzer von Kaspersky Anti-Virus können den Technischen Support-Service in Anspruch nehmen. Verwenden Sie die Funktion **Support**, um zu erfahren, wo Sie technische Unterstützung erhalten können.

Mit Hilfe der entsprechenden Links gelangen Sie zum Benutzerforum für die Kaspersky-Lab-Produkte oder zu einer Übersicht über häufige Fragen, die bei der Problemlösung behilflich sein können. Außerdem finden Sie auf dieser Webseite ein spezielles Formular, mit dem Sie eine Fehlermeldung oder Rückmeldung über die Arbeit des Programms an den Technischen Support senden können.

Zusätzlich steht Ihnen ein technischer Online-Support zur Verfügung. Natürlich können Sie sich auch telefonisch an unsere Mitarbeiter wenden, wenn Sie bei der Arbeit mit Kaspersky Anti-Virus Hilfe benötigen.

INSTALLATION VON KASPERSKY ANTI-VIRUS 6.0

Es bestehen mehrere Möglichkeiten, um Kaspersky Anti-Virus 6.0 für Windows Server MP4 auf dem Computer zu installieren:

- lokale Installation – Installation der Anwendung auf einem einzelnen Computer. Für den Start und die Durchführung der Installation ist der direkte Zugriff auf diesen Computer erforderlich. Für die lokale Installation stehen zwei Modi zur Auswahl:
  - interaktiver Modus mit Hilfe des Installationsassistenten für das Programm (s. Abschnitt "Installation mit Hilfe des Installationsassistenten" auf S. 17). Dieser Modus erfordert während der Installation bestimmte Aktionen des Benutzers.
  - Silent-Modus. In diesem Fall wird die Programminstallation aus der Befehlszeile gestartet und erfordert während des Installationsvorgangs keine weiteren Aktionen des Benutzers (s. Abschnitt "3.3. Installation der Anwendung aus der Befehlszeile" auf S. 21).
- Remote-Installation – Installation der Anwendung auf Netzwerkcomputern. Die Installation erfolgt im Remote-Modus vom Arbeitsplatz des Administrators aus und unter Einsatz von:
  - Programmkomplex Kaspersky Administration Kit (s. "Handbuch zur Einführung von Kaspersky Administration Kit");
  - Domain-Gruppenaufgaben für Microsoft Windows Server 2000/2003 (s. Abschnitt "Installation über Gruppenrichtlinienobjekt-Editor (Group Policy Object)" auf S. 21).

Es wird empfohlen, vor dem Beginn der Installation von Kaspersky Anti-Virus (auch bei der Remote-Installation) alle laufenden Anwendungen zu schließen.

IN DIESEM ABSCHNITT

INSTALLATION MIT HILFE DES INSTALLATIONSASSISTENTEN

Um Kaspersky Anti-Virus auf Ihrem Computer zu installieren, starten Sie die Distributionsdatei auf der Produkt-CD.

Die Installation der Anwendung von einer Distribution, die aus dem Internet heruntergeladen wurde, ist mit der Installation der Anwendung von einer Distributions-CD vollkommen identisch.

Der Installer ist wie ein Assistent aufgemacht. In jedem Fenster stehen verschiedene Schaltflächen, um den Installationsvorgang zu verwalten. Es folgt eine kurze Beschreibung:

- **Weiter** – Vorgang wird angenommen und es geht weiter zum nächsten Schritt im Installationsvorgang.

- **Zurück** – Rückkehr zum vorangegangenen Schritt der Installation.
- **Abbrechen** – Installation des Produkts abbrechen.
- **Fertig** – Installationsvorgang des Programms auf dem Computer wird beendet.

Betrachten wir die einzelnen Schritte des Installationsvorgangs ausführlich.

SCHRITT 1. ÜBERPRÜFEN DES SYSTEMS AUF DIE INSTALLATIONSVORAUSSETZUNGEN

Bevor das Programm auf Ihrem Computer installiert wird, werden das installierte Betriebssystem und die vorhandenen Service Packs auf Übereinstimmung mit den Softwarevoraussetzungen für die Installation überprüft. Außerdem wird überprüft, ob die erforderlichen Programme auf dem Computer vorhanden sind und ob Sie über die zur Programminstallation notwendigen Rechte verfügen.

Sollte eine bestimmte Voraussetzung nicht erfüllt sein, dann erscheint eine entsprechende Meldung auf dem Bildschirm. Es wird empfohlen, vor der Installation der Kaspersky-Lab-Anwendung die erforderlichen Programme und mit Hilfe des Diensts **Windows Update** die fehlenden Service Packs zu installieren.

SCHRITT 2. STARTFENSTER DES INSTALLATIONSVORGANGS

Wenn Ihr System alle Voraussetzungen erfüllt, erscheint sofort nach dem Start der Distributionsdatei auf dem Bildschirm das Startfenster, das Informationen über den Beginn der Installation von Kaspersky Anti-Virus auf dem Computer enthält.

Zum Fortsetzen der Installation klicken Sie auf die Schaltfläche **Weiter**. Klicken Sie auf **Abbrechen**, um die Installation zu verwerfen.

SCHRITT 3. LESEN DES LIZENZVERTRAGS

Das folgende Fenster des Installationsprogramms enthält den Lizenzvertrag, der zwischen Ihnen und Kaspersky Lab geschlossen wird. Bitte lesen Sie den Vertrag aufmerksam. Wenn Sie allen Punkten des Vertrags zustimmen, wählen Sie die Variante **Ich akzeptiere die Bedingungen des Lizenzvertrags** und klicken Sie auf die Schaltfläche **Weiter**. Die Installation wird fortgesetzt.

Zum Ablehnen klicken Sie auf die Schaltfläche **Abbrechen**.

SCHRITT 4. INSTALLATIONSORDNER WÄHLEN

Beim nächsten Schritt der Installation von Kaspersky Anti-Virus wird festgelegt, in welchem Ordner des Computers die Anwendung installiert werden soll. Der Standardpfad lautet:

- **<Laufwerk> → Program Files → Kaspersky Lab → Kaspersky Anti-Virus 6.0 für Windows Server MP4** – für 32-Bit-Systeme.
- **<Laufwerk> → Program Files (x86) → Kaspersky Lab → Kaspersky Anti-Virus 6.0 für Windows Server MP4 MP4** – für 64-Bit-Systeme.

Sie können einen anderen Ordner wählen. Klicken Sie dazu auf die Schaltfläche **Durchsuchen** und wählen Sie im standardmäßigen Auswahlfenster einen Ordner aus oder geben Sie den Pfad des Ordners im entsprechenden Eingabefeld an.

Falls Sie den vollständigen Pfad des Ordners manuell angeben, beachten Sie, dass er aus maximal 200 Zeichen bestehen und keine Sonderzeichen enthalten darf.

Zum Fortsetzen der Installation klicken Sie auf die Schaltfläche **Weiter**.

SCHRITT 5. PROGRAMMEINSTELLUNGEN EINER VORGÄNGERVERSION VERWENDEN

Auf dieser Etappe können Sie festlegen, ob für die Arbeit des Programms die Schutzeinstellungen und die Programm-Datenbanken verwendet werden sollen, die auf Ihrem Computer bei der Deinstallation einer älteren Version von Kaspersky Anti-Virus 6.0 gespeichert wurden.

Es wird detailliert betrachtet, wie sich die oben beschriebenen Optionen nutzen lassen.

Wenn auf Ihrem Computer zuvor eine ältere Version (Build) von Kaspersky Anti-Virus installiert war und Sie bei der Deinstallation die Programm-Datenbanken auf dem Computer gespeichert haben, können Sie diese in der zu installierenden Version verwenden. Setzen Sie dazu das Häkchen im Kontrollkästchen ☑ **Programm-Datenbanken**. Die ursprünglich mitgelieferten Datenbanken werden nicht auf den Server kopiert.

Um die Schutzparameter zu verwenden, die Sie in der vorherigen Version angepasst und auf dem Computer gespeichert haben, aktivieren Sie das Kontrollkästchen ☑ **Funktionsparameter der Anwendung**.

SCHRITT 6. INSTALLATIONSTYP AUSWÄHLEN

Auf dieser Etappe können Sie festlegen, in welchem Umfang die Anwendung auf Ihrem installiert werden soll. Es sind zwei Varianten für die Installation vorgesehen:

Vollständig. In diesem Fall werden alle Komponenten von Kaspersky Anti-Virus auf dem Server installiert. Nähere Informationen über die weiteren Installationsschritte s. Schritt 8.

Benutzerdefiniert. In diesem Fall können Sie die Programmkomponenten auswählen, die auf dem Server installiert werden sollen. Details s. Schritt.7.

Klicken Sie auf die entsprechende Schaltfläche, um einen Installationstyp auszuwählen.

SCHRITT 7. PROGRAMMKOMPONENTEN FÜR INSTALLATION AUSWÄHLEN

Dieser Schritt des Installationsassistenten wird nur bei der **benutzerdefinierten** Programminstallation ausgeführt.

Bei der benutzerdefinierten Installation müssen Sie die Komponenten von Kaspersky Anti-Virus festlegen, die installiert werden sollen. Standardmäßig sind folgende Elemente für die Installation ausgewählt: Datei-Anti-Virus, die Komponente zur Virensuche, Connector zum Administrationsagenten für die Fernverwaltung der Anwendung über Kaspersky Administration Kit.

Um eine Komponente zur anschließenden Installation auszuwählen, wird durch Linksklick auf das Symbol neben dem Komponentennamen das Menü geöffnet und der Punkt **Die Komponente wird auf der lokalen Festplatte installiert** gewählt. Informationen über die Schutzfunktion der ausgewählten Komponente und über den für ihre Installation auf der Festplatte erforderlichen Platz werden im unteren Bereich des Installationsfensters genannt.

Genaue Angaben über den freien Platz auf den Festplatten Ihres Computers erhalten Sie durch Klick auf die Schaltfläche **Laufwerk**. Die Informationen werden im folgenden Fenster angezeigt.

Für Komponenten, die nicht installiert werden sollen, wählen Sie im Kontextmenü die Variante **Die Komponente wird nicht verfügbar sein**. Beachten Sie, dass Sie auf den Schutz vor einer ganzen Reihe gefährlicher Programme verzichten, wenn Sie eine bestimmte Komponente nicht installieren.

Klicken Sie auf die Schaltfläche **Weiter**, nachdem Sie die zur Installation gewünschten Komponenten gewählt haben. Um zur Liste mit den standardmäßig zu installierenden Komponenten zurückzugehen, klicken Sie auf die Schaltfläche **Zurück**.

SCHRITT 9. NACH ANDEREN ANTIVIREN-ANWENDUNGEN SUCHEN

Auf dieser Etappe erfolgt die Suche nach anderen auf dem Server installierten Antiviren-Produkten (einschließlich Kaspersky-Lab-Produkte), deren gleichzeitige Verwendung mit Kaspersky Anti-Virus zu Konflikten führen kann.

Beim Erkennen von solchen Programmen auf dem Server wird die Liste auf dem Bildschirm angezeigt. Ihnen wird deren Deinstallation vorgeschlagen, bevor Sie mit der Installation fortsetzen.

Unter der Liste der gefundenen Antiviren-Anwendungen können Sie wählen, ob sie automatisch oder manuell entfernt werden sollen. Nur Kaspersky-Lab-Produkte werden automatisch gelöscht.

Zum Fortsetzen der Installation klicken Sie auf die Schaltfläche **Weiter**.

SCHRITT 10. PROGRAMMINSTALLATION ABSCHLIEßEND VORBEREITEN

Auf dieser Etappe können Sie die Installation des Programms auf dem Server abschließend vorbereiten.

Bei der Erstinstallation von Kaspersky Anti-Virus 6.0 sollte das Kontrollkästchen ☑ **Installationsprozess schützen** nicht entfernt werden. Falls während der Programminstallation Fehler auftreten sollten, erlaubt es dieser Modulschutz, die Installation auf korrekte Weise rückgängig zu machen. Wenn die Anwendung nicht zum ersten Mal installiert wird, ist es empfehlenswert, dieses Kontrollkästchen zu entfernen.

Bei einer Remote-Installation des Programms auf dem Computer über **Windows Remote Desktop** wird empfohlen, das Häkchen im Kontrollkästchen ☑ **Installationsvorgang schützen** zu entfernen. Andernfalls kann es sein, dass der Installationsvorgang nicht oder fehlerhaft durchgeführt wird.

Falls Sie möchten, dass den Ausnahmen automatisch die von Microsoft für Server empfohlenen Ausnahmen hinzugefühgt werden, aktivieren Sie das Kontrollkästchen ☑ **Von Microsoft vorgegebenen Bereiche aus dem Untersuchungsbereich ausschließen**.

Falls Sie möchten, dass der Pfad von avp.com zur Umgebungsvariable %PATH% nach der Installation hinzuzufügt wurde, aktivieren Sie das Kontrollkästchen ☑ **Pfad zu avp.com zur Umgebungsvariable %PATH% hinzufügen**.

Zum Fortsetzen der Installation klicken Sie auf die Schaltfläche **Weiter**.

Während Komponenten von Kaspersky Anti-Virus installiert werden, die der Kontrolle des Netzwerkverkehrs dienen, werden bestehende Netzwerkverbindungen getrennt. Die Mehrzahl der getrennten Verbindungen wird nach einiger Zeit wiederhergestellt.

SCHRITT 11. INSTALLATIONSVORGANG ABSCHLIEßEN

Das Fenster **Installation fertigstellen** enthält Informationen über den Abschluss des Installationsvorgangs von Kaspersky Anti-Virus auf dem Server.

Klicken Sie auf die Schaltfläche **Weiter**, um den Konfigurationsassistenten zu starten.

Wenn für den korrekten Abschluss der Installation ein Neustart des Computers erforderlich ist, erscheint ein entsprechender Hinweis auf dem Bildschirm.

INSTALLATION MIT HILFE DES INSTALLATIONSASSISTENTEN AUS DER BEFEHLSZEILE

- *Um Kaspersky Anti-Virus 6.0 für Windows Server MP4 zu installieren, geben Sie in der Befehlszeile ein:*

```
msiexec /i <Paketname>
```

Der Installationsassistent wird gestartet (s. Abschnitt "Installation mit Hilfe des Installationsassistenten" auf S. 17). Zum Abschluss der Programminstallation ist ein Neustart des Computers erforderlich.

- *Um die Anwendung im Silent-Modus (ohne Start des Installationsassistenten) zu installieren, geben Sie folgende Befehlszeile ein:*

```
msiexec /i <Paketname> /qn
```

In diesem Fall muss der Computer nach Abschluss der Installation manuell neu gestartet werden. Damit ein automatischer Neustart erfolgt, geben Sie folgende Befehlszeile ein:

```
msiexec /i <Paketname> ALLOWREBOOT=1 /qn
```

Beachten Sie, dass ein automatischer Neustart des Computers nur im Silent-Installationsmodus ausgeführt werden kann (mit dem Schlüssel /qn).

- *Um die Anwendung zu installieren und dabei ein für die Programmdeinstallation vorgesehenes Kennwort festzulegen, geben Sie ein:*

  `msiexec /i <Paketname> KLUNINSTPASSWD=******` – für die Programminstallation im interaktiven Modus.

  `msiexec /i <Paketname> KLUNINSTPASSWD=****** /qn` – für die Programminstallation im Silent-Modus ohne Neustart des Computer.

  `msiexec /i <Paketname> KLUNINSTPASSWD=****** ALLOWREBOOT=1 /qn` – für die Programminstallation im Silent-Modus mit anschließendem Neustart des Computer.

Bei der Installation von Kaspersky Anti-Virus im Silent-Modus wird das Lesen folgender Dateien unterstützt: Datei setup.ini, die allgemeine Installationsparameter für das Programm enthält, Konfigurationsdatei *install.cfg* (s. Abschnitt "Import von Schutzparametern" auf S. 115) und Lizenzschlüsseldatei. Beachten Sie, dass sich diese Dateien im gleichen Ordner befinden müssen, wie die Distribution von Kaspersky Anti-Virus.

INSTALLATION ÜBER GRUPPENRICHTLINIENOBJEKT-EDITOR (GROUP POLICY OBJECT)

Mit Hilfe des **Gruppenrichtlinienobjekt-Editors** können Sie Kaspersky Anti-Virus auf den zu einer Domäne gehörenden Workstations eines Unternehmens installieren, aktualisieren und löschen, ohne Kaspersky Administration Kit zu verwenden.

PROGRAMMINSTALLATION

- *Gehen Sie folgendermaßen vor, um Kaspersky Anti-Virus zu installieren:*

1. Erstellen Sie einen gemeinsamen Netzwerkordner auf dem Computer, der als Domänencontroller funktioniert, und speichern Sie dort die Distribution von Kaspersky Anti-Virus im Format *.msi*.

   Zusätzlich können in diesem Verzeichnis folgende Elemente abgelegt werden: Datei *setup.ini*, die eine Liste der Installationsparameter für Kaspersky Anti-Virus enthält, Konfigurationsdatei *install.cfg* (s. Abschnitt "Import von Schutzparametern" auf S. 115) und Schlüsseldatei.

2. Öffnen Sie den **Gruppenrichtlinienobjekt-Editor** über die Standardkonsole MMC (Details über die Arbeit mit dem Editor siehe Hilfesystem für Microsoft Windows Server).

3. Erstellen Sie ein neues Paket. Wählen Sie dazu in der Konsolenstruktur **Gruppenrichtlinienobjekt/ Computerkonfiguration/ Software-Einstellungen/ Software-Installation** und verwenden Sie im Kontextmenü den Befehl **Neu/ Paket**.

   Geben Sie im folgenden Fenster den Pfad des gemeinsamen Netzwerkordners an, der die Distribution von Kaspersky Anti-Virus enthält. Wählen Sie im Fenster **Bereitstellung des Programms** den Parameter **Zugewiesen** und klicken Sie auf die Schaltfläche **OK**.

Die Gruppenrichtlinie wird auf allen Workstations übernommen, wenn sich die Computer zum nächsten Mal in der Domäne anmelden. Dadurch wird Kaspersky Anti-Virus auf allen Computern installiert.

BESCHREIBUNG DER PARAMETER DER DATEI SETUP.INI

Die Datei *setup.ini*, die sich im Distributionsordner von Kaspersky Anti-Virus befindet, wird bei der Installation im Silent-Modus über die Befehlszeile oder den Gruppenrichtlinienobjekt-Editor verwendet. Diese Datei enthält folgende Parameter:

[Setup] – allgemeine Installationsparameter für das Programm.

- **InstallDir=**<Pfad des Installationsordners für das Programm>.
- **Reboot=yes|no** – Gibt an, ob beim Abschluss der Installation ein Neustart des Computers erfolgen soll (standardmäßig wird kein Neustart ausgeführt).
- **SelfProtection=yes|no** – Gibt an, ob bei der Installation der Selbstschutz für Kaspersky Anti-Virus aktiviert werden soll (der Selbstschutz ist standardmäßig aktiviert).

[Components] – Auswahl der zu installierenden Programmkomponenten. Wenn diese Gruppe keine Elemente enthält, wird die Anwendung vollständig installiert.

- **FileMonitor=yes|no** – Installation der Komponente Datei-Anti-Virus.

[Tasks] – Aufgaben von Kaspersky Anti-Virus aktivieren. Wenn keine Aufgabe angegeben wird, werden nach der Installation alle Aufgaben aktiviert. Werden eine oder mehrere Aufgaben angegeben, dann werden die nicht markierten Aufgaben nicht aktiviert.

- **ScanMyComputer=yes|no** – Aufgabe zur vollständigen Untersuchung.
- **ScanStartup=yes|no** – Aufgabe zur schnellen Untersuchung.
- **Scan=yes|no** – Untersuchungsaufgabe.
- **Updater=yes|no** – Aufgabe zum Update der Datenbanken und Programm-Module.

Anstelle des Werts **yes** können die Werte 1, on, enable oder enabled verwendet werden, anstelle des Wertes **no** – 0, off, disable oder disabled.

UPDATE DER PROGRAMMVERSION

➧ *Gehen Sie folgendermaßen vor, um die Version von Kaspersky Anti-Virus zu aktualisieren:*

1. Speichern Sie die Distribution, die das Update für Kaspersky Anti-Virus enthält (im Format .msi) in einen gemeinsamen Netzwerkordner.

2. Öffnen Sie den **Gruppenrichtlinienobjekt-Editor** und erstellen, wie oben beschrieben, Sie ein neues Paket.

3. Markieren Sie das neue Paket in der Liste und verwenden Sie im Kontextmenü den Befehl **Eigenschaften**. Gehen Sie im Eigenschaftenfenster auf die Registerkarte **Update** und geben Sie das Paket an, das die Distribution der Vorgängerversion von Kaspersky Anti-Virus enthält. Um die aktuelle Version von Kaspersky Anti-Virus zu installieren und die Schutzparameter beizubehalten, wählen Sie die Variante zur Installation über das vorhandene Paket.

Die Gruppenrichtlinie wird auf allen Workstations übernommen, wenn sich die Computer zum nächsten Mal in der Domäne anmelden.

Beachten Sie, dass auf Computern mit dem Betriebssystem Microsoft Windows 2000 Server das Update von Kaspersky Anti-Virus über den Gruppenrichtlinienobjekt-Editor nicht unterstützt wird.

DEINSTALLATION DER ANWENDUNG

➡ *Gehen Sie folgendermaßen vor, um Kaspersky Anti-Virus zu deinstallieren:*

1. Öffnen Sie das **Gruppenrichtlinienobjekt-Editor**.

2. Wählen Sie in der Konsolenstruktur **Gruppenrichtlinienobjekt / Computerkonfiguration/ Software-Einstellungen/ Software-Installation**.

   Markieren Sie in der Liste der Pakete das Paket für Kaspersky Anti-Virus, öffnen Sie das Kontextmenü und wählen Sie den Befehl **Alle Aufgaben/ Löschen**.

Wählen Sie im Dialogfenster **Anwendungen löschen** die Variante **Diese Anwendung sofort von den Computern aller Benutzer löschen**, damit Kaspersky Anti-Virus beim nächsten Neustart des Computers deinstalliert wird.

ERSTE SCHRITTE

Bei der Entwicklung von Kaspersky Anti-Virus bestand eine der Hauptaufgaben der Spezialisten von Kaspersky Lab in der optimalen Konfiguration aller Programmeinstellungen.

Um die Benutzerfreundlichkeit zu erhöhen, wurden die Schritte zur grundlegenden Konfiguration in einem Konfigurationsassistenten zusammengefasst, der am Ende der Programminstallation gestartet wird. Im Rahmen des Assistenten können Sie das Programm aktivieren, Einstellungen für das Update und den Start von Untersuchungsaufgaben vornehmen, und den Zugriff auf das Programm mit Hilfe eines Kennworts beschränken.

Wir empfehlen Ihnen, nach der Installation und dem Start des Programms auf Ihrem Computer folgende Aktionen vorzunehmen:

- Bewertung des aktuellen Schutzstatus (s. Abschnitt "Sicherheitsverwaltung" auf S. 30), um sicherzustellen, dass Kaspersky Anti-Virus den Schutz auf der erforderlichen Stufe gewährleistet.
- Aktualisierung des Programms (s. S. "Programm-Update" auf S. 29) (sofern das Update nicht mit Hilfe des Konfigurationsassistenten oder sofort nach der Installation automatisch erfolgt ist).
- Untersuchung des Servers (s. Abschnitt "Virenuntersuchung des Computers" auf S. 28) auf Viren.

IN DIESEM ABSCHNITT

KONFIGURATIONSASSISTENT

Der Konfigurationsassistent für das Programm wird am Ende der Installation gestartet. Seine Aufgabe ist es, Sie bei der ersten Konfiguration der Programmparameter zu unterstützen und dabei die Besonderheiten der Aufgaben Ihres Computers zu berücksichtigen.

Der Konfigurationsassistent besitzt das Aussehen einen Microsoft Windows-Programmassistenten (Windows Wizard) und besteht aus einer Folge von Fenstern (Schritten). Zur Navigation zwischen den Fenstern dienen die Schaltflächen **Weiter** und **Zurück**, zum Abschluss der Arbeit des Assistenten die Schaltfläche **Fertig** stellen. Die Arbeit des Assistenten kann auf einer beliebigen Etappe durch Klick auf die Schaltfläche **Abbrechen** beendet werden.

Um die Anwendung vollständig auf dem Computer zu installieren, müssen alle Schritte des Assistenten ausgeführt werden. Wenn der Assistent aus irgendwelchen Gründen abgebrochen wird, werden bereits festgelegte Parameterwerte

nicht gespeichert. Bei einem späteren Versuch, die Arbeit mit der Anwendung zu beginnen, wird der Konfigurationsassistent wieder von vorne gestartet, was bedeutet, dass die Parameter erneut angepasst werden müssen.

VERWENDUNG VON OBJEKTEN, DIE IN DER VORHERGEHENDEN VERSION GESPEICHERT WURDEN

Dieses Fenster des Assistenten erscheint, wenn die Anwendung über die vorhergehende Version des Kaspersky Anti-Virus installiert wird. Es wird Ihnen angeboten, die in der vorhergehenden Version verwendeten Daten auszuwählen, die auf die neue Version übertragen werden sollen. Dazu zählen Quarantäne- und Backup-Objekte sowie Schutzeinstellungen.

Aktivieren Sie die entsprechenden Kontrollkästchen, um diese Daten in der neuen Version des Programms zu verwenden.

PROGRAMM AKTIVIEREN

Bei der Programmaktivierung wird durch die Installation einer Schlüsseldatei eine Lizenz registriert. Auf Grundlage der Lizenz ermittelt die Anwendung, ob Rechte für die Programmnutzung bestehen und welche Nutzungsdauer dafür gilt.

Der Schlüssel enthält Dienstinformationen, die für die volle Funktionsfähigkeit von Kaspersky Anti-Virus erforderlich sind, sowie zusätzliche Angaben:

- Informationen über den Support (von wem und wo man technische Unterstützung erhalten kann).
- Bezeichnung, Nummer und Gültigkeitsdauer der Lizenz.

Abhängig davon, ob Sie über eine Schlüsseldatei verfügen oder diese zuerst von einem Kaspersky-Lab-Server herunterladen müssen, bestehen folgende Möglichkeiten für die Aktivierung von Kaspersky Anti-Virus:

- Online-Aktivierung (auf S. 26). Wählen Sie diese Aktivierungsmethode, wenn Sie eine kommerzielle Programmversion erworben und Sie einen Aktivierungscode erhalten haben. Auf Basis dieses Codes bekommen Sie eine Schlüsseldatei, die Ihnen während der gesamten Laufzeit der Lizenz den Zugriff auf die volle Funktionsfähigkeit des Programms bietet.
- Aktivierung einer Testversion (auf S. 26). Wählen Sie diese Aktivierungsvariante, wenn Sie eine Testversion des Programms installieren möchten, bevor Sie über den Kauf einer kommerziellen Version entscheiden. Sie erhalten eine kostenlose Schlüsseldatei, deren Gültigkeitsdauer durch die Lizenz der Testversion dieses Programms beschränkt ist.
- Aktivierung mit einer vorhandenen Schlüsseldatei (s. Abschnitt "Aktivierung mit Hilfe einer Schlüsseldatei" auf S. 26). Aktivieren Sie die Anwendung mit einer bereits vorhandenen Schlüsseldatei für Kaspersky Anti-Virus 6.0.
- Das Programm später aktivieren. Bei der Auswahl dieser Variante wird die Aktivierung von Kaspersky Anti-Virus übersprungen. Das Programm wird auf Ihrem Computer installiert und Sie können alle Programmfunktionen außer dem Update nutzen. (Das Programm kann nach der Installation nur einmal aktualisiert werden.) Die Variante **Das Programm später aktivieren** ist nur beim ersten Start des Aktivierungsassistenten verfügbar. Bei nachfolgenden Starts des Assistenten steht, falls die Anwendung bereits aktiviert wurde, die Variante **Schlüsseldatei löschen** zur Verfügung.

Wenn eine der ersten beiden Varianten gewählt wird, erfolgt die Programmaktivierung über den Webserver von Kaspersky Lab. Dafür ist eine Internetverbindung erforderlich. Prüfen Sie vor Beginn der Aktivierung die Parameter der Netzwerkverbindung im Fenster, das mit der Schaltfläche **LAN-Einstellungen** geöffnet wird. Weitere Informationen über die Konfiguration der Netzwerkparameter erhalten Sie bei Ihren Systemadministrator oder Internetprovider.

Ist bei der Installation keine Internetverbindung vorhanden, dann kann die Aktivierung später über die Programmoberfläche vorgenommen werden. Außerdem besteht die Möglichkeit, von einem anderen Computer aus ins Internet zu gehen, sich auf der Support-Webseite von Kaspersky Lab anzumelden und mit Hilfe des Aktivierungscodes eine Schlüsseldatei herunterzuladen.

Sie können die Anwendung auch über Kaspersky Administration Kit aktivieren. Dazu muss eine Aufgabe zur Installation einer Schlüsseldatei (s. S. 129) erstellt werden (Details siehe Handbuch zu "Kaspersky Administration Kit").

SIEHE AUCH

ONLINE-AKTIVIERUNG

Die Online-Aktivierung beruht auf der Eingabe des Aktivierungscodes, den Sie per E-Mail erhalten, wenn Sie Kaspersky Anti-Virus über das Internet kaufen. Wurde die Anwendung in einer CD-Box gekauft, dann ist der Aktivierungscode auf dem Umschlag der Installations-CD angegeben.

EINGABE DES AKTIVIERUNGSCODES

Auf dieser Etappe ist die Eingabe eines Aktivierungscodes erforderlich. Der Aktivierungscode besteht aus einer durch Bindestriche getrennten Ziffernfolge mit vier Blöcken zu je fünf Ziffern ohne Leerzeichen. Beispiel, 11111-11111-11111-11111. Beachten Sie bitte, dass der Code in lateinischen Buchstaben eingegeben werden muss.

Geben Sie im unteren Bereich des Fensters Ihre Kontaktinformationen ein: Nachname, Vorname, E-Mail, Land und Wohnort. Diese Informationen können erforderlich sein, um einen registrierten Benutzer zu identifizieren, wenn beispielsweise seine Lizenzdaten verloren gegangen sind oder gestohlen wurden. In diesem Fall können Sie auf Basis der Kontaktinformationen einen anderen Aktivierungscode erhalten.

DOWNLOAD EINER SCHLÜSSELDATEI

Der Konfigurationsassistent baut eine Verbindung mit den Kaspersky-Lab-Servern im Internet auf und sendet Ihre Anmeldedaten (Aktivierungscode, Kontaktinformationen) an die Server. Nach dem Aufbau einer Verbindung mit dem Server werden der Aktivierungscode und die Vollständigkeit der Kontaktinformationen geprüft. Wenn der Aktivierungscode die Überprüfung besteht, erhält der Assistent eine Schlüsseldatei, die automatisch installiert wird. Der Aktivierungsvorgang wird abgeschlossen und es erscheint ein Fenster mit ausführlichen Informationen über die erworbene Lizenz.

Wenn der Aktivierungscode die Überprüfung nicht bestanden hat, erscheint eine entsprechende Meldung auf dem Bildschirm. In diesem Fall sollten Sie sich an die Firma wenden, bei der Sie Kaspersky Anti-Virus gekauft haben.

Wenn die zulässige Anzahl der Aktivierungen für diesen Aktivierungscode überschritten wurde, erscheint eine entsprechende Meldung auf dem Bildschirm. Der Aktivierungsvorgang wird abgebrochen und das Programm schlägt Ihnen vor, sich an den Support von Kaspersky Lab zu wenden.

TRIALVERSION AKTIVIEREN

Wählen Sie diese Aktivierungsvariante, wenn Sie eine Testversion von Kaspersky Anti-Virus installieren möchten, bevor Sie über den Kauf einer kommerziellen Version entscheiden. Sie erhalten eine kostenlose Lizenz, deren Gültigkeitsdauer durch den Lizenzvertrag der Testversion dieser Anwendung beschränkt ist. Nach Ablauf der Lizenz ist die Aktivierung einer Testlizenz nicht mehr möglich.

AKTIVIERUNG MIT HILFE EINER SCHLÜSSELDATEI

Wenn Sie eine Schlüsseldatei besitzen, können Sie Kaspersky Anti-Virus damit aktivieren. Verwenden Sie dazu die Schaltfläche **Durchsuchen** und wählen Sie eine Datei mit der Erweiterung *.key* aus.

Nach der erfolgreichen Installation des Schlüssels erscheinen im unteren Bereich des Fensters Informationen über die Lizenz: Nummer, Typ (kommerziell, Test usw.), Gültigkeitsdauer der Lizenz, sowie Anzahl der Computer, für die die Lizenz gültig ist.

AKTIVIERUNG ABSCHLIEßEN

Der Konfigurationsassistent informiert Sie über den erfolgreichen Abschluss der Aktivierung von Kaspersky Anti-Virus. Außerdem werden Informationen über die Lizenz angezeigt: Nummer, Typ (kommerziell, für Beta-Test, Test usw.), Gültigkeitsdauer der Lizenz, sowie Anzahl der Computer, für die die Lizenz gültig ist.

ANPASSEN DER PARAMETER FÜR DAS UPDATE

Die Qualität des Schutzes Ihres Computers ist unmittelbar vom rechtzeitigen Download der Updates für die Datenbanken und Programm-Module abhängig. In diesem Fenster des Assistenten können Sie den Modus für das Programm-Update wählen und Einstellungen für den Zeitplan vornehmen:

- **Automatisch**. Kaspersky Anti-Virus prüft in festgelegten Zeitabständen, ob an der Updatequelle ein neues Updatepaket vorhanden ist. Die Häufigkeit der Überprüfung kann während Viren-Epidemien steigen und unter gewöhnlichen Umständen sinken. Wenn neue Updates vorhanden sind, lädt Kaspersky Anti-Virus sie herunter und installiert sie auf dem Computer. Dieser Modus wird standardmäßig verwendet.

- **Alle 2 Stunden** (Das Intervall ist von den Zeitplaneinstellungen abhängig). Das Update wird automatisch nach einem festgelegten Zeitplan gestartet. Der Zeitplan wird in dem Fenster angepasst, das durch Klick auf die Schaltfläche **Ändern** geöffnet wird.

- **Manuell**. In diesem Fall starten Sie das Programm-Update manuell.

Beachten Sie, dass die Datenbanken und Programm-Module, die in der Distribution enthalten sind, zum Zeitpunkt der Programminstallation bereits veraltet sein können. Wir empfehlen deshalb, die aktuellen Programm-Updates herunterzuladen. Klicken Sie dazu auf die Schaltfläche **Jetzt aktualisieren**. In diesem Fall lädt Kaspersky Anti-Virus die erforderlichen Updates von den Updateseiten im Internet herunter und installiert sie auf dem Computer.

Wenn Sie die Updateparameter anpassen möchten (Netzwerkparameter festlegen, Ressource wählen, von der das Update erfolgt, Start der Aktualisierung unter einem bestimmten Benutzerkonto konfigurieren, Dienst zur Update-Verteilung aktivieren), klicken Sie auf die Schaltfläche **Einstellungen**.

ANPASSEN DES ZEITPLANS FÜR DIE VIRENUNTERSUCHUNG

Die Suche nach schädlichen Objekten in vorgegebenen Untersuchungsbereichen ist eine der wichtigsten Aufgaben für den Schutz des Computers.

Bei der Installation von Kaspersky Anti-Virus werden standardmäßig mehrere Untersuchungsaufgaben erstellt. In diesem Fenster bietet Ihnen der Assistent an, den Startmodus für die Untersuchungsaufgaben festzulegen:

Vollständige Suche

Ausführliche Untersuchung des Systems. Standardmäßig werden folgende Objekte untersucht: Systemspeicher, Objekte, die beim Systemstart gestartet werden, Systemwiederherstellung, Mail-Datenbanken, Festplatten, Wechseldatenträger und Netzlaufwerke. Die Zeitplaneinstellungen können im Fenster geändert werden, das mit der Schaltfläche **Ändern** geöffnet wird.

Schnelle Suche

Virenuntersuchung der Objekte, die beim Start des Betriebssystems geladen werden. Die Zeitplaneinstellungen können im Fenster geändert werden, das mit der Schaltfläche **Ändern** geöffnet wird.

KONTROLLE DES ZUGRIFFS AUF DAS PROGRAMM.

Ein Server kann von mehreren Benutzern verwendet werden, u.a. von Benutzern, deren Fertigkeiten im Umgang mit Computern möglicherweise nicht ausreichend sind. Außerdem können Schadprogramme versuchen, den Schutz auszuschalten. Deshalb besteht die Möglichkeit, den Zugriff auf Kaspersky Anti-Virus durch ein Kennwort zu beschränken. Das Kennwort erlaubt es, das Programm vor Versuchen zum unerlaubten Ausschalten des Schutzes oder zum Ändern der Programmeinstellungen zu schützen.

Um den Kennwortschutz zu verwenden, kreuzen Sie das Kontrollkästchen ☑ **Kennwortschutz aktivieren** an und füllen Sie die Felder **Kennwort** und **Kennwort bestätigen** aus.

Geben Sie darunter den Bereich an, auf den sich die Zugriffsbeschränkung beziehen soll:

- ◉ **Alle Operationen (außer Gefahrenmeldungen)**. Das Kennwort wird bei jeder beliebigen Aktion abgefragt, die vom Benutzer mit dem Programm initiiert wird. Die einzige Ausnahme bilden Meldungen über den Fund gefährlicher Objekte.
- ◉ **Nur für ausgewählte Aktionen**:
  - ☑ **Programmparameter anpassen** – Wenn der Benutzer versucht, die Einstellungen von Kaspersky Anti-Virus zu ändern, wird das Kennwort abgefragt.
  - ☑ **Programm beenden** – Kennwortabfrage beim Versuch des Benutzers, die Arbeit des Programms zu beenden.
  - ☑ **Schutzkomponenten deaktivieren und Untersuchungsaufgaben beenden** – Kennwortabfrage beim Versuch eines Benutzers, den Datei-Anti-Virus zu deaktivieren oder eine Aufgabe zur Virensuche zu beenden.
  - ☑ **Richtlinie von Kaspersky Administration Kit deaktivieren** – Kennwortabfrage beim Versuch des Benutzers, den Computer aus dem Gültigkeitsbereich von Richtlinien und Gruppenaufgaben (bei der Arbeit über Kaspersky Administration Kit) auszuschließen.
  - ☑ **Bei Deinstallation der Anwendung** – Kennwortabfrage beim Versuch des Benutzers, die Anwendung vom Computer zu entfernen.

ABSCHLUSS DES KONFIGURATIONSASSISTENTEN

Das letzte Fenster des Assistenten informiert darüber, dass die Installation und Konfiguration von Kaspersky Anti-Virus erfolgreich verlaufen sind. Sie können die Anwendung sofort starten. Aktivieren Sie dazu das Kontrollkästchen ☑ **Anwendung starten**.

Wenn bei der Installation Probleme aufgetreten sind, z.B. wenn inkompatible Versionen anderer Antiviren-Programme gefunden wurden, kann ein Neustart des Computers erforderlich sein.

VIRENUNTERSUCHUNG DES COMPUTERS

Die Autoren schädlicher Programme geben sich große Mühe, die Aktivität ihrer Programme zu verheimlichen. Deshalb kann es sein, dass Sie die Existenz von Malware auf Ihren Computer nicht bemerken.

Bei der Installation von Kaspersky Anti-Virus wird automatisch die Aufgabe **Schnelle Suche** ausgeführt. Diese Aufgabe dient der Suche und Neutralisierung von schädlichen Programmen in Objekten, die beim Hochfahren des Betriebssystems geladen werden.

Die Spezialisten von Kaspersky Lab empfehlen, zusätzlich die Aufgabe **Vollständige Suche** auszuführen.

➧ *Gehen Sie folgendermaßen vor, um eine Untersuchungsaufgabe zu starten / zu beenden:*

1. Öffnen Sie das Programmhauptfenster.

2. Wählen Sie auf der linken Fensterseite den Abschnitt **Virensuche** (**Vollständige Suche**, **Schnelle Suche**).

3. Klicken Sie auf die Schaltfläche **Untersuchung ausführen**, um die Untersuchung zu starten. Klicken Sie auf den Schaltfläche Untersuchung **beenden** falls eine laufende Aufgabe beendet werden soll.

PROGRAMM-UPDATE

Für das Update von Kaspersky Anti-Virus ist eine bestehende Internetverbindung erforderlich.

Zum Lieferumfang von Kaspersky Anti-Virus gehören Datenbanken mit Bedrohungssignaturen. Zum Zeitpunkt der Programminstallation können die Programm-Datenbanken bereits veraltet sein, da Datenbanken und Programm-Module regelmäßig von Kaspersky Lab aufgefrischt werden.

Im Rahmen des Konfigurationsassistenten für das Programm können Sie einen Startmodus für das Update auswählen. Kaspersky Anti-Virus prüft in der Grundeinstellung automatisch, ob auf den Kaspersky-Lab-Servern neue Updates vorhanden sind. Wenn auf dem Server neue Updates vorhanden sind, führt Kaspersky Anti-Virus im Hintergrundmodus den Download und die Installation der Updates durch.

Um den Serverschutz auf dem aktuellen Stand zu halten, wird empfohlen, Kaspersky Anti-Virus sofort nach der Installation zu aktualisieren.

➧ *Gehen Sie folgendermaßen vor, um Kaspersky Anti-Virus manuell zu aktualisieren:*

1. Öffnen Sie das Programmhauptfenster.

2. Wählen Sie auf der linken Fensterseite den Abschnitt **Update**.

3. Klicken Sie auf die Schaltfläche **Update ausführen**.

LIZENZVERWALTUNG

Die Möglichkeit zur Benutzung von Kaspersky Anti-Virus wird durch das Vorhandensein einer Lizenz bestimmt. Eine Lizenz erhalten Sie durch den Kauf des Produkts. Sie berechtigt Sie ab dem Tag der Aktivierung zur Benutzung der Anwendung.

Wenn keine Lizenz vorhanden ist und keine Testversion der Anwendung aktiviert wurde, funktioniert Kaspersky Anti-Virus in einem Modus, in dem das Update nur ein einziges Mal möglich ist. Danach werden keine neuen Updates mehr ausgeführt.

Wenn eine Testversion der Anwendung aktiviert wurde, wird Kaspersky Anti-Virus nach dem Ablauf der Testlizenz nicht mehr funktionieren.

Bei Ablauf der Gültigkeitsdauer einer kommerziellen Lizenz bleibt die Funktionalität des Programms unter Ausnahme der Updatemöglichkeit für die Programm-Datenbanken erhalten. Sie können Ihren Computer mit Hilfe der Untersuchungsaufgaben weiterhin untersuchen und die Schutzkomponenten verwenden, allerdings nur mit den Datenbanken, die bei Ablauf der Lizenz aktuell waren. Demzufolge können wir Ihnen keinen hundertprozentigen Schutz vor neuen Viren garantieren, die nach dem Gültigkeitsende des Schlüssels für das Programm auftreten.

Um eine Infektion Ihres Computers durch neue Viren zu verhindern, empfehlen wird Ihnen, die Lizenz für die Benutzung von Kaspersky Anti-Virus zu verlängern. Die Anwendung informiert Sie darüber zwei Wochen vor Ablauf der Lizenz. Innerhalb eines bestimmten Zeitraums wird bei jedem Programmstart eine entsprechende Meldung auf dem Bildschirm angezeigt.

Der Abschnitt **Lizenz** des Hauptfensters von Kaspersky Anti-Virus enthält die wichtigsten Informationen über die verwendete Lizenz (aktive Lizenz und, falls installiert, Reservelizenz): Typ (kommerziell, Test, für Beta-Test), maximale Anzahl der Computer, Gültigkeitsdauer der Lizenz und Anzahl der bis zum Ablauf verbleibenden Tage. Um nähere Informationen über die Lizenz zu erhalten, verwenden Sie den Link für den entsprechenden Lizenztyp.

Zu den Bedingungen des Lizenzvertrags über die Nutzung des Programms gelangen Sie über die Schaltfläche **Lizenzvertrag lesen**.

Um eine Lizenz zu entfernen, verwenden Sie die Schaltfläche **Hinzufügen** / **Löschen** und folgen Sie den Anweisungen des Assistenten.

Kaspersky Lab führt in regelmäßigen Zeitabständen Aktionen durch, bei denen Lizenzen für unsere Produkte zu besonders günstigen Preisen angeboten werden. Verfolgen Sie unsere Aktionen auf der Internetseite von Kaspersky Lab im Abschnitt **Produkte** → **Aktionen und Sonderangebote**.

Gehen Sie folgendermaßen vor, um eine Lizenz zu kaufen oder deren Gültigkeit zu verlängern:

1. Kaufen Sie eine neue Schlüsseldatei oder einen Aktivierungscode. Verwenden Sie dazu die Schaltfläche **Lizenz kaufen** (falls die Anwendung noch nicht aktiviert wurde) oder **Lizenz verlängern**. Auf unserer automatisch geöffneten Webseite erhalten Sie umfassende Informationen darüber, zu welchen Bedingungen Sie im Internet-Shop von Kaspersky Lab oder bei einem autorisierten Händler einen Schlüssel kaufen können. Beim Kauf über einen Internet-Shop wird Ihnen nach Eingang der Bezahlung per E-Mail an die im Bestellformular angegebene Adresse eine Schlüsseldatei oder ein Aktivierungscode für das Programm zugeschickt.

2. Aktivieren Sie die Anwendung. Verwenden Sie dazu die Schaltfläche **Hinzufügen / Löschen** im Abschnitt **Lizenz** des Programmhauptfensters oder den Befehl **Aktivieren** im Kontextmenü des Programms. Dadurch wird der Aktivierungsassistent gestartet.

SICHERHEITSVERWALTUNG

Über das Auftreten von Problemen im Computerschutz informiert der Schutzstatus des Computers (s. Abschnitt "Programmhauptfenster" auf S. 36) durch eine Veränderung der Farbe des Schutzstatussymbols und der Leiste, auf der sich das Symbol befindet. Wenn im Schutz Probleme auftreten, sollten diese umgehend behoben werden.

Abbildung 1. Aktueller Schutzstatus des Computers

Über den Link **Korrigieren** (s. Abbildung oben) gelangen Sie zum Sicherheitsassistenten (s. Abbildung unten), der eine Liste der aufgetretenen Probleme und entsprechende Lösungsmöglichkeiten bietet.

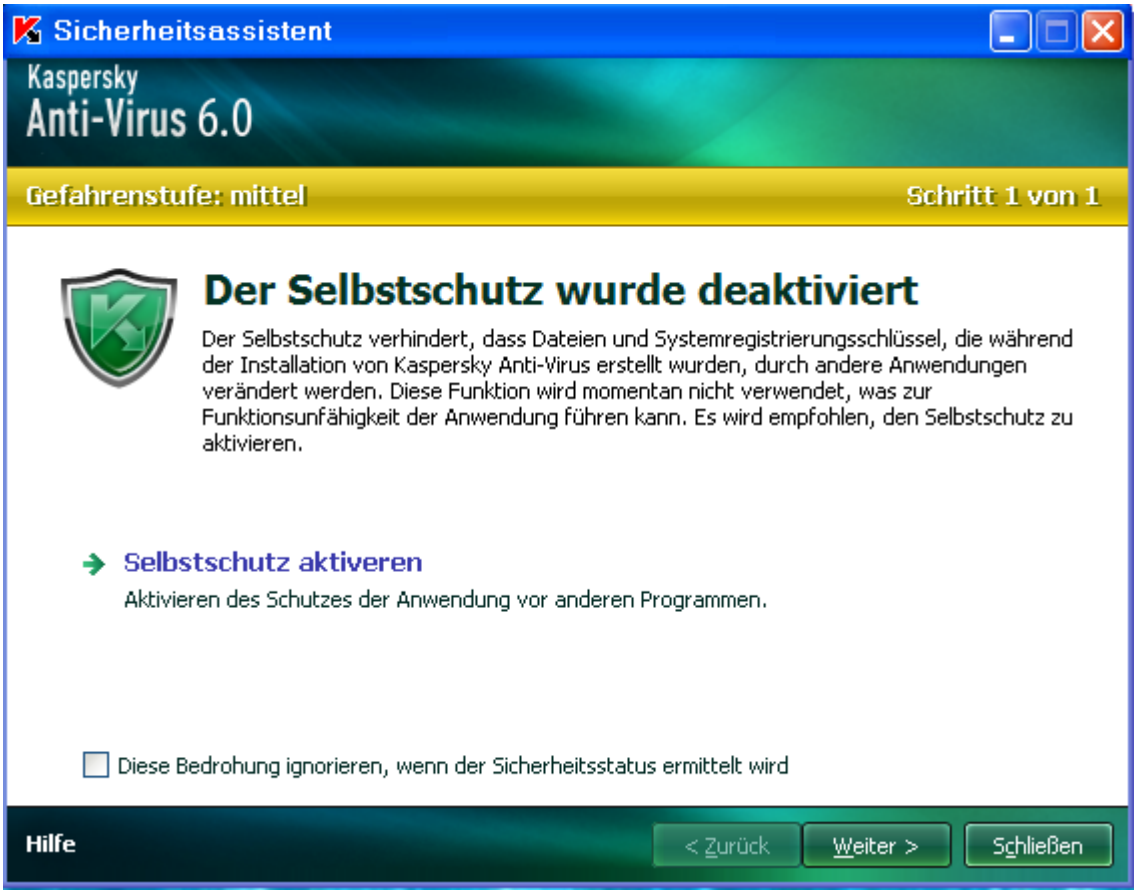


Abbildung 2. Beheben von Sicherheitsproblemen

Sie können eine Liste der vorhandenen Probleme ansehen. Die Reihenfolge der Probleme entspricht der Priorität, nach der sie gelöst werden sollten: Zu Beginn stehen die wichtigsten Probleme mit rotem Statussymbol, danach folgen die weniger wichtigen mit gelbem Statussymbol und zum Schluss informative Meldungen. Für jedes Problem ist eine ausführliche Beschreibung vorhanden und folgende Aktionen werden angeboten:

- *Sofort beheben*. Mit Hilfe der entsprechenden Links können Sie zur sofortigen Neutralisierung der Probleme übergehen, was der empfohlenen Aktion entspricht.

- *Behebung aufschieben*. Wenn das sofortige Beheben eines Problems aufgrund bestimmter Umstände nicht möglich ist, kann diese Aktion aufgeschoben werden und Sie können später dazu zurückkehren. Aktivieren Sie das Kontrollkästchen ☑ **Diese Bedrohung ignorieren, wenn der Sicherheitsstatus ermittelt wird**, damit die Bedrohung den aktuellen Schutzstatus nicht beeinflusst.

  Beachten Sie, dass diese Möglichkeit für kritische Probleme nicht vorgesehen ist. Dazu gehören beispielsweise die Existenz nicht neutralisierter Schädlinge, Störungen bei der Arbeit einer oder mehrerer Komponenten, und beschädigte Programmdateien. Solche Probleme sollten unverzüglich behoben werden.

SCHUTZ ANHALTEN

Das Anhalten des Schutzes bedeutet, dass Datei-Anti-Virus für einen bestimmten Zeitraum deaktivert wird.

➡ *Gehen Sie folgendermaßen vor, um die Arbeit von Kaspersky Anti-Virus anzuhalten:*

1. Im ählen Sie im Kontextmenü des Programms den Punkt **Schutz anhalten**.

2. Wählen Sie im folgenden Fenster **Schutz anhalten** den Zeitraum fest, nach dem der Schutz wieder aktiviert werden soll.

PROBLEMBEHEBUNG. TECHNISCHER SUPPORT FÜR BENUTZER

Wenn bei der Verwendung von Kaspersky Anti-Virus Probleme aufgetreten sind, prüfen Sie bitte zuerst, ob das Hilfesystem oder die Wissensdatenbank von Kaspersky Lab (http://support.kaspersky.de) eine Lösung für Ihr Problem bieten. Die *Wissensdatenbank* ist ein Abschnitt der Webseite des Technischen Support-Services und enthält Tipps über die Arbeit mit Kaspersky-Lab-Produkten und Antworten auf häufige Fragen. Versuchen Sie, auf dieser Ressource eine Antwort auf Ihre Frage oder eine Lösung für Ihr Problem zu finden.

➧ *Gehen Sie folgendermaßen vor, um die Wissensdatenbank zu verwenden:*

1. Öffnen Sie das Programmhauptfenster.
2. Klicken Sie im unteren Bereich des Fensters auf den Link **Support**.
3. Klicken Sie im folgenden Fenster **Support** auf den Link **Technischer Support**.

Eine weitere Ressource, die Informationen über die Arbeit mit der Anwendung bietet, ist das Benutzerforum für Kaspersky-Lab-Produkte. Diese Ressource ist ebenfalls ein Abschnitt der Webseite des Technischen Support Services und enthält Fragen, Kommentare und Vorschläge von Programmbenutzern. Sie können die wichtigsten Themen des Forums kennen lernen, eigene Beiträge über das Programm schreiben oder Antworten auf Ihre Frage suchen.

➧ *Gehen Sie folgendermaßen vor, um die Webseite des Benutzerforums zu öffnen:*

1. Öffnen Sie das Programmhauptfenster.
2. Klicken Sie im unteren Bereich des Fensters auf den Link **Support**.
3. Klicken Sie im folgenden Fenster **Support** auf den Link **Benutzerforum**.

Wenn Sie im Hilfesystem, in der Wissensdatenbank oder im Benutzerforum keine Lösung für Ihr Problem finden können, empfehlen wir Ihnen, sich an den Technischen Support von Kaspersky Lab zu wenden.

ERSTELLEN EINER PROTOKOLLDATEI

Nach der Installation von Kaspersky Anti-Virus können bei der Arbeit des Betriebssystems oder bestimmter Programme Störungen auftreten. Dies deutet höchstwahrscheinlich auf einen Konflikt der Anwendung mit einem auf Ihrem Computer installierten Programm oder mit auf Ihrem Computer vorhandenen Treibern hin. Damit die Support-Spezialisten von Kaspersky Lab Sie bei der Lösung Ihres Problems unterstützen können, kann es sein, dass der Support Sie auffordert, eine Protokolldatei zu erstellen.

➧ *Gehen Sie folgendermaßen vor, um eine Protokolldatei zu erstellen:*

1. Öffnen Sie das Programmhauptfenster.
2. Klicken Sie im unteren Bereich des Programmfensters auf den Link **Support**.
3. Klicken Sie im folgenden Fenster **Support** auf den Link **Protokollierung**.
4. Verwenden Sie im folgenden Fenster **Informationen für den Support** die Dropdown-Liste im Block **Protokollierung**, um ein Protokollierungsniveau auszuwählen. Das Tracing-Niveau wird von dem Support-Spezialisten angegeben. Sollte diese Angabe des Supports fehlen, dann empfohlen, das Tracing-Niveau **500** einzustellen.
5. Klicken Sie auf die Schaltfläche **Aktivieren**, um den Protokollierungsvorgang zu starten.

6. Wiederholen Sie die Situation, in der das Problem aufgetreten ist.

7. Klicken Sie auf die Schaltfläche **Deaktivieren**, um den Protokollierungsvorgang zu beenden.

PROGRAMMPARAMETER ANPASSEN

Dem schnellen Zugriff auf die Parameter von Kaspersky Anti-Virus 6.0 dient das Konfigurationsfenster des Programms (s. S. 75), das aus dem Hauptfenster mit der Schaltfläche **Einstellungen** geöffnet.

BERICHTE ÜBER DIE PROGRAMMARBEIT. DATENVERWALTUNG

Die Arbeit jeder Komponente von Kaspersky Anti-Virus und die Ausführung jeder Untersuchungs- und Updateaufgabe werden in einem Bericht (s. S. 90) protokolliert. Um zur Anzeige der Berichte zu wechseln, verwenden Sie die Schaltfläche **Berichte**, die sich unten rechts im Hauptfenster befindet.

Die *Datenverwaltung der Anwendung* umfasst Objekte, die von Kaspersky Anti-Virus in der Quarantäne (s. S. 92) oder im Backup (s. S. 93) gespeichert wurden. Mit der Schaltfläche **Gefunden** können Sie das Fenster **Datenspeicher** öffnen, in dem Sie mit diesem Objekten arbeiten können.

PROGRAMMOBERFLÄCHE

Kaspersky Anti-Virus verfügt über eine einfache und komfortable Oberfläche. In diesem Kapitel werden die wichtigsten Elemente der Oberfläche ausführlich beschrieben:

- Symbol im Infobereich der Taskleiste.
- Kontextmenü.
- Hauptfenster.
- Meldungen.
- Konfigurationsfenster von Kaspersky Anti-Virus.

IN DIESEM ABSCHNITT

SYMBOL IM INFOBEREICH DER TASKLEISTE.

Sofort nach der Installation von Kaspersky Anti-Virus erscheint sein Symbol im Infobereich der Taskleiste.

Das Symbol ist ein spezieller Indikator für die Arbeit von Kaspersky Anti-Virus. Es informiert über den Schutzstatus und zeigt eine Reihe wichtiger Aktionen, die vom Programm ausgeführt werden.

Das aktive (farbige) Symbol, bedeutet, dass der Serverschutz aktiviert ist. Ist das Symbol inaktiv (schwarzweiß), dann wurde der Schutz deaktiviert.

Je nach der momentan ausgeführten Operation verändert sich das Symbol von Kaspersky Anti-Virus:

- Eine Datei wird untersucht, die Sie oder ein Programm öffnen, speichern oder starten.
- Die Datenbanken und Module von Kaspersky Anti-Virus werden aktualisiert.
- Bei der Arbeit einer Komponente von Kaspersky Anti-Virus ist eine Störung aufgetreten.

Das Symbol bietet außerdem Zugriff auf die wichtigsten Elemente der Programmoberfläche: Kontextmenü und Hauptfenster.

Um das Kontextmenü zu öffnen, klicken Sie mit der rechten Maustaste auf das Programmsymbol.

Um das Hauptfenster von Kaspersky Anti-Virus zu öffnen, klicken Sie mit der linken Maustaste auf das Programmsymbol.

KONTEXTMENÜ

Das Kontextmenü bietet Zugriff auf die wichtigsten Schutzaufgaben.

Das Menü von Kaspersky Anti-Virus enthält folgende Punkte:

- **Vollständige Suche –** Starten der vollständigen Untersuchung Ihres Computers auf das Vorhandensein schädlicher Objekte. Dadurch werden die Objekte auf allen Laufwerken einschließlich der Wechseldatenträger untersucht.
- **Virensuche –** Zur Auswahl von Objekten und zum Start der Virensuche wechseln. Standardmäßig enthält die Liste bestimmte Objekte wie beispielsweise Systemspeicher, Autostart-Objekte, Mailboxen, alle Serverlaufwerke u.a. Sie können die Liste ergänzen, Untersuchungsobjekte auswählen und eine Virenuntersuchung starten.
- **Update –** Starten der Aktualisierung der Module und Datenbanken von Kaspersky Anti-Virus und der Installation der Updates auf Ihrem Computer.
- **Aktivieren –** Zur Aktivierung des Programms wechseln. Um den Status eines registrierten Benutzers zu erhalten, auf dessen Basis Ihnen die volle Funktionsfähigkeit der Anwendung und die Leistungen des Technischen Support-Services zur Verfügung gestellt werden, ist es erforderlich, Kaspersky Anti-Virus zu aktivieren. Dieser Menüpunkt ist nur vorhanden, wenn das Programm noch nicht aktiviert wurde.
- **Einstellungen** – Zur Anzeige und Konfiguration der Funktionsparameter von Kaspersky Anti-Virus wechseln.
- **Kaspersky Anti-Virus –** Hauptfenster des Programms öffnen.
- **Schutz anhalten / Schutz aktivieren** – Datei-Anti-Virus vorübergehend deaktivieren / aktivieren. Dieser Menüpunkt besitzt keinen Einfluss auf das Programm-Update und die Ausführung von Untersuchungsaufgaben.
- **Richtlinie deaktivieren / Richtlinie aktivieren** – Vorübergehendes Deaktivieren / Aktivieren einer Richtlinie bei der Arbeit der Anwendung über Kaspersky Administration Kit. Mit diesem Menüpunkt kann der Computer aus dem Gültigkeitsbereich von Richtlinien und Gruppenaufgaben ausgeschlossen werden. Diese Funktion ist durch ein Kennwort (s. Abschnitt "Kontrolle des Zugriffs auf das Programm" auf S. 86) geschützt. Der Menüpunkt ist nur vorhanden, wenn ein Kennwort festgelegt wurde.
- **Über das Programm** – Öffnen des Informationsfensters über das Programm.
- **Beenden** – Kaspersky Anti-Virus beenden (Bei Auswahl dieses Menüpunkts wird die Anwendung aus dem Arbeitsspeicher des Computers entfernt).

Abbildung 3. Kontextmenü

Wenn eine Untersuchungsaufgabe läuft, wird ihr Name im Kontextmenü mit einer Prozentangabe des Ausführungsergebnisses angezeigt. Durch die Auswahl der Aufgabe gelangen Sie in das Berichtsfenster mit den aktuellen Ausführungsergebnissen.

PROGRAMMHAUPTFENSTER

Das Programmhauptfenster lässt sich bedingt in drei Bereiche aufteilen:

- Der obere Bereich des Fensters informiert über den aktuellen Schutzstatus Ihres Computers.

Abbildung 4. Aktueller Schutzstatus des Computers

Es gibt drei Varianten für den Schutzstatus. Jeder Status wird durch eine Farbe signalisiert. Die Farben entsprechen den Signalen einer Ampel. Grün bedeutet, dass der Schutz Ihres Computers dem erforderlichen Niveau entspricht. Gelb und Rot signalisieren, dass in den Einstellungen oder bei der Arbeit von Kaspersky Anti-Virus bestimmte Sicherheitsbedrohungen vorliegen. Als Bedrohung gelten nicht nur schädliche Programme, sondern beispielsweise auch veraltete Programm-Datenbanken.

Vorhandene Sicherheitsrisiken sollten umgehend behoben werden. Verwenden Sie den Link **Korrigieren** (s. Abbildung oben), um ausführliche Informationen darüber zu erhalten und die Bedrohungen schnell zu beheben.

- Die linke Seite des Fensters bietet schnellen und bequemen Zugriff auf alle Programmfunktionen, auf die Ausführung von Aufgaben zur Virensuche oder zum Update, u.a.

Abbildung 5. Linke Seite des Hauptfensters

- Die rechte Seite des Fensters enthält Informationen über die auf der linken Seite gewählte Programmfunktion, erlaubt es, die Parameter aller Funktionen anzupassen, bietet Werkzeuge zum Ausführen von Aufgaben zur Virensuche, zum Update-Download, u.a.

Abbildung 6. Rechte Seite des Hauptfensters

Außerdem können Sie folgende Werkzeuge verwenden:

- Schaltfläche **Einstellungen** – in das Programmkonfigurationsfenster (s. S. 75) wechseln.
- Link **Hilfe** – zum Hilfesystem für Kaspersky Anti-Virus wechseln.
- Schaltfläche **Gefunden** - zur Datenverwaltung (s. S. 90) des Programms wechseln.
- Schaltfläche **Berichte** – zu den Berichten über die Arbeit der Programmkomponenten (s. S. 90) wechseln.
- Link **Support** – Fenster mit Informationen über das System und mit Links zu Informationsressourcen von Kaspersky Lab (s. S. 32) (Webseite des Technischen Supports, Forum) öffnen.

MELDUNGEN

Wenn bei der Arbeit von Kaspersky Anti-Virus bestimmte Ereignisse eintreten, werden Sie durch Popupmeldungen über dem Programmsymbol im Infobereich der Taskleiste von Microsoft Windows darüber informiert.

In Abhängigkeit davon, welche Relevanz das Ereignis für die Computersicherheit besitzt, sind folgende Arten von Meldungen möglich:

- **Alarm**. Ein Ereignis mit kritischer Priorität ist eingetreten. Beispiele: Ein Virus wurde gefunden. Die sofortige Entscheidung über das weitere Vorgehen ist erforderlich. Dieser Meldungstyp besitzt die Farbe Rot.

- **Warnung**. Ein potentiell gefährliches Ereignis hat sich ereignet. Beispiele: Ein möglicherweise infiziertes Objekt wurde gefunden. Es muss entschieden werden, inwieweit das Ereignis nach Ihrem Ermessen gefährlich ist. Dieser Meldungstyp besitzt die Farbe Gelb.

- **Informationen**. Diese Meldung informiert über ein Ereignis, das keine vorrangige Priorität besitzt. Dieser Meldungstyp besitzt die Farbe Grün.

SIEHE AUCH

Arten von Meldungen 106

PROGRAMMKONFIGURATIONSFENSTER

Das Konfigurationsfenster von Kaspersky Anti-Virus kann aus dem Hauptfenster geöffnet werden. Klicken Sie dazu im oberen Fensterbereich auf die Schaltfläche **Einstellungen**.

Das Konfigurationsfenster entspricht in seiner Struktur dem Hauptfenster:

- Die linke Seite des Fensters bietet schnellen und bequemen Zugriff auf die Einstellungen von Datei-Anti-Virus, der Untersuchungsaufgaben und der Updateaufgabe sowie auf die Dienstfunktionen der Anwendung.

- Die rechte Seite des Fensters enthält eine Liste von Parametern für den auf der linken Seite ausgewählte Punkt (Datei-Anti-Virus, Aufgabe usw.).

SIEHE AUCH

Programmparameter anpassen 75

ANTIVIREN-SCHUTZ FÜR DAS DATEISYSTEM DES COMPUTERS

Datei-Anti-Virus erlaubt es, das Dateisystem des Computers vor einer Infektion zu schützen. Die Komponente wird beim Hochfahren des Betriebssystems gestartet, befindet sich ständig im Arbeitsspeicher des Computers und untersucht alle Dateien, die geöffnet, gespeichert und gestartet werden.

In der Grundeinstellung untersucht Datei-Anti-Virus nur neue oder veränderte Dateien. Die Untersuchung von Dateien erfolgt mit einer bestimmten Auswahl von Parametern, die als Sicherheitsstufe bezeichnet wird. Beim Fund von Bedrohungen führt Datei-Anti-Virus die festgelegte Aktion aus.

Das Schutzniveau für die Dateien und den Speicher auf Ihrem Computer wird durch folgende Gruppen von Parametern definiert:

- Parameter, die den geschützten Bereich festlegen
- Parameter für die Untersuchungsmethoden für Dateien
- Parameter für die Untersuchung zusammengesetzter Dateien (einschließlich der Untersuchung großer zusammengesetzter Dateien)
- Parameter für den Untersuchungsmodus
- Parameter, die es erlauben, die Arbeit der Komponente anzuhalten (nach Zeitplan; während der Arbeit bestimmter Programme).

Gehen Sie folgendermaßen vor, um die Funktionsparameter von Datei-Anti-Virus anzupassen:

1. Öffnen Sie das Programmhauptfenster und klicken Sie im oberen Bereich des Fensters auf die Schaltfläche **Einstellungen**.
2. Nehmen Sie im folgenden Fenster die erforderlichen Änderungen in den Einstellungen der Komponente vor.

IN DIESEM ABSCHNITT

ALGORITHMUS FÜR DIE ARBEIT DER KOMPONENTE

Datei-Anti-Virus wird beim Hochfahren des Betriebssystems gestartet, befindet sich ständig im Arbeitsspeicher des Computers und untersucht alle Dateien, die geöffnet, gespeichert und gestartet werden.

Standardmäßig untersucht Datei-Anti-Virus nur neue oder veränderte Dateien, d.h. Dateien, die seit dem letzten Zugriff hinzugefügt oder verändert wurden. Die Untersuchung einer Datei erfolgt nach folgendem Algorithmus:

1. Die Komponente fängt den Zugriff des Benutzers oder eines bestimmten Programms auf eine beliebige Datei ab.

2. Datei-Anti-Virus prüft, ob in den Datenbanken iChecker und iSwift Informationen über die abgefangene Datei vorhanden sind. Auf Basis dieser Informationen wird entschieden, ob eine Untersuchung der Datei erforderlich ist.

Die Untersuchung umfasst folgende Aktionen:

- Die Datei wird auf das Vorhandensein von Viren untersucht. Objekte werden auf Basis der Programm-Datenbanken erkannt. Die Datenbanken enthalten eine Beschreibung aller momentan bekannten Schadprogramme, Bedrohungen und Netzwerkangriffe sowie entsprechende Desinfektionsmethoden.

- Aufgrund der Analyseergebnisse bestehen folgende Varianten für das Verhalten von Kaspersky Anti-Virus:

  a. Wenn in der Datei schädlicher Code gefunden wird, sperrt der Datei-Anti-Virus die Datei, speichert eine Kopie im *Backup* und versucht, die Desinfektion durchzuführen. Bei erfolgreicher Desinfektion erhält der Benutzer Zugriff auf die E-Mail. Wenn die Desinfektion fehlschlägt, wird die Datei gelöscht.

b. Wenn in der Datei ein Code gefunden wird, der Ähnlichkeit mit schädlichem Code besitzt, jedoch keine hundertprozentige Sicherheit darüber besteht, wird die Datei der Desinfektion unterzogen und in den *Quarantänespeicher* verschoben.

c. Wenn in der Datei kein schädlicher Code gefunden wird, wird der Zugriff darauf sofort freigegeben.

Beim Fund eines infizierten oder möglicherweise infizierten Objekts werden Sie vom Programm darüber informiert. Die Meldung erfordert die Auswahl einer Aktion:

- Bedrohung in die Quarantäne verschieben, um sie später mit Hilfe aktualisierter Datenbanken zu untersuchen und zu verarbeiten.
- Objekt löschen.
- Überspringen, wenn Sie absolut sicher sind, dass das Objekt unschädlich ist.

SIEHE AUCH

Antiviren-Schutz für das Dateisystem des Computers.....39

ÄNDERN DER SICHERHEITSSTUFE

Unter Sicherheitsstufe wird eine vordefinierte Auswahl von Parametern für Datei-Anti-Virus verstanden. Die Spezialisten von Kaspersky Lab haben drei Sicherheitsstufen vordefiniert. Sie treffen selbst eine Entscheidung über die Auswahl der Sicherheitsstufe, wobei die Arbeitsbedingungen und die aktuelle Situation berücksichtigt werden sollten.

- Wenn die Wahrscheinlichkeit einer Infektion des Computers sehr hoch ist, sollte unbedingt die hohe Sicherheitsstufe gewählt werden.
- Die empfohlene Stufe bietet ein ausgewogenes Verhältnis zwischen Leistung und Sicherheit. Sie ist für die meisten Situationen geeignet.
- Bei der Arbeit in einer geschützten Umgebung (z.B. Firmennetzwerk mit zentralem Sicherheitssystem) und bei der Arbeit mit ressourcenaufwändigen Anwendungen sollte die niedrige Sicherheitsstufe verwendet werden.

Es wird empfohlen, vor der Auswahl der niedrigen Sicherheitsstufe die vollständige Untersuchung des Computers mit der hohen Sicherheitsstufe vorzunehmen.

Wenn keine der vordefinierten Stufen Ihren Anforderungen entspricht, können Sie die Funktionsparameter von Datei-Anti-Virus anpassen. Dadurch ändert sich der Name der Sicherheitsstufe in **Benutzerdefiniert**. Um die standardmäßigen Einstellungen der Komponente wiederherzustellen, wählen Sie eine der vordefinierten Stufen.

➡ *Gehen Sie folgendermaßen vor, um die festgelegte Sicherheitsstufe für Datei-Anti-Virus zu ändern:*

1. Öffnen Sie das Programmhauptfenster und klicken Sie im oberen Bereich des Fensters auf die Schaltfläche **Einstellungen**.
2. Wählen Sie im folgenden Fenster die gewünschte Sicherheitsstufe aus.

AKTION FÜR GEFUNDENE OBJEKTE ÄNDERN

Datei-Anti-Virus kann gefundenen Objekten aufgrund des Untersuchungsergebnisses einen der folgenden Status zuweisen:

- Status eines der schädlichen Programme (beispielsweise *Virus*, *trojanisches Programm*).

- *möglicherweise infiziert*, wenn sich aufgrund der Untersuchung nicht eindeutig feststellen lässt, ob das Objekt infiziert ist oder nicht. Das bedeutet, dass in der Datei die Codefolge eines unbekannten Virus oder der modifizierte Code eines bekannten Virus gefunden wurde.

Wenn Kaspersky Anti-Virus bei der Virenuntersuchung einer Datei infizierte oder verdächtige Objekte findet, sind die weiteren Operationen, die Datei-Anti-Virus ausführt, vom Status des Objekts und von der festgelegten Aktion abhängig.

Standardmäßig werden alle infizierten Dateien der Desinfektion unterzogen und alle möglicherweise infizierten Dateien in die Quarantäne verschoben.

Alle verfügbaren Aktionen werden in der folgenden Tabelle genannt.

GEWÄHLTE AKTION	WAS GESCHIEHT BEIM FUND EINES GEFÄHRLICHEN OBJEKTS?
☑ **Desinfizieren** ☐ **Löschen, wenn Desinfektion nicht möglich**	Der Zugriff auf das Objekt wird gesperrt und es erfolgt ein Desinfektionsversuch, wobei eine Kopie des Objekts im Backup gespeichert wird. Bei erfolgreicher Desinfektion wird das Objekt für den Benutzer zur Arbeit freigegeben. Kann das Objekt nicht desinfiziert werden, wird es in die Quarantäne verschoben. Informationen darüber werden im Bericht aufgezeichnet. Später kann versucht werden, das Objekt zu desinfizieren.
☑ **Desinfizieren** ☑ **Löschen, wenn Desinfektion nicht möglich**	Der Zugriff auf das Objekt wird gesperrt und es erfolgt ein Desinfektionsversuch, wobei eine Kopie des Objekts im Backup gespeichert wird. Bei erfolgreicher Desinfektion wird das Objekt für den Benutzer zur Arbeit freigegeben. Kann das Objekt nicht desinfiziert werden, wird es gelöscht.
☐ **Desinfizieren** ☑ **Löschen**	Datei-Anti-Virus blockiert den Zugriff auf das Objekt und löscht es.
☑ **Den Benutzer sperren für ... Stunden**	Die aktuelle Verbindung des Benutzerkontos mit dem Server sperren, wenn versucht wird, ein infiziertes oder möglicherweise infiziertes Objekt zu kopieren. Diese Aktion kann zusätzlich zu den Aktionen angewandt werden, die mit der Objektbearbeitung (Desinfektion oder Löschen) verbunden sind. Hinweis: Wenn ein Benutzer die Sitzung beendet und sich erneut am System anmeldet, betrachtet Kaspersky Anti-Virus dies als eine andere Verbindung und die Blockade wird aufgehoben.

Bevor ein Desinfektionsversuch erfolgt oder ein Objekt gelöscht wird, legt Kaspersky Anti-Virus eine Sicherungskopie des Objekts an und speichert diese im Backup. Dadurch wird erlaubt, das Objekt bei Bedarf wiederherzustellen oder später zu desinfizieren.

Objekte mit dem Status *möglicherweise infiziert* werden ohne vorherigen Desinfektionsversuch in die Quarantäne verschoben.

➧ *Gehen Sie folgendermaßen vor, um die festgelegte Aktion für gefundene Objekte zu ändern:*

1. Öffnen Sie das Programmhauptfenster und klicken Sie im oberen Bereich des Fensters auf die Schaltfläche **Einstellungen**.

2. Wählen Sie im folgenden Fenster die Komponente **Datei-Anti-Virus** und klicken Sie auf die Schaltfläche **Einstellungen**.

3. Wählen Sie im folgenden Fenster im Block **Aktion** die entsprechende Aktion aus.

SCHUTZBEREICH FESTLEGEN

Unter dem Schutzbereich wird nicht nur der Ort der Untersuchungsobjekte verstanden, sondern auch der Typ der zu untersuchenden Dateien. Kaspersky Anti-Virus untersucht standardmäßig nur .potentiell infizierbare Dateien, die von beliebigen Festplatten, Wechseldatenträgern und Netzlaufwerken aus gestartet werden.

Sie können den Schutzbereich erweitern oder einschränken, indem Sie Untersuchungsobjekte hinzufügen / entfernen oder die Typen der zu untersuchenden Dateien ändern. Sie können beispielsweise nur exe-Dateien, die von Netzlaufwerken aus gestartet werden, untersuchen lassen. Allerdings sollten Sie sicherstellen, dass eine Einschränkung des Schutzbereichs nicht zu einem Sicherheitsrisiko für den Computer führt.

Bei der Auswahl des Dateityps muss Folgendes beachtet werden:

- Es gibt eine Reihe von Dateiformaten, für die das Risiko des Eindringens von schädlichem Code und der späteren Aktivierung relativ gering ist (z.B. *txt*). Es gibt auch Formate, die ausführbaren Code enthalten oder enthalten können (*exe*, *dll*, *doc*). Das Risiko, dass schädlicher Code in solche Dateien eindringt und später aktiviert wird, ist relativ hoch.

- Ein Angreifer kann einen Virus in einer Datei mit der Erweiterung *txt* an Ihren Computer senden, obwohl es sich in Wirklichkeit um eine ausführbare Datei handelt, die in eine *txt*-Datei umbenannt wurde. Wenn die Variante **Dateien nach Erweiterung untersuchen** gewählt wurde, wird eine solche Datei bei der Untersuchung übersprungen. Wurde die Variante **Dateien nach Format untersuchen** gewählt, so analysiert Kaspersky Anti-Virus ungeachtet der Erweiterung die Kopfzeile der Datei, wodurch sich ergibt, dass die Datei das Format *exe* besitzt. Eine solche Datei wird der sorgfältigen Virenuntersuchung unterzogen.

Durch die Angabe des Typs der zu untersuchenden Dateien definieren Sie das Format, die Größe und die Laufwerke der Dateien, die beim Öffnen, Ausführen und Speichern auf Viren untersucht werden sollen.

Zur Vereinfachung der Konfiguration werden alle Dateien in zwei Gruppen eingeteilt: *einfache* und *zusammengesetzte*. Einfache Dateien enthalten kein anderes Objekt (z.B. eine txt-Datei). Zusammengesetzte Objekte können mehrere Objekte umfassen, die wiederum jeweils mehrere Anhänge enthalten können. Beispiele für solche Objekte sind Archive, Dateien, die Makros, Tabellen, Nachrichten mit Anlagen usw. enthalten.

Beachten Sie, dass Datei-Anti-Virus nur jene Dateien auf Viren untersucht, die zu dem erstellten Schutzbereich gehören. Dateien, die nicht in diesem Bereich fallen, werden ohne Untersuchung zur Arbeit freigegeben. Dadurch steigt das Risiko einer Infektion des Computers!

➡ *Gehen Sie folgendermaßen vor, um die Liste der Untersuchungsobjekte zu ändern:*

1. Öffnen Sie das Programmhauptfenster und klicken Sie im oberen Bereich des Fensters auf die Schaltfläche **Einstellungen**.

2. Wählen Sie im folgenden Fenster die Komponente **Datei-Anti-Virus** und klicken Sie auf die Schaltfläche **Einstellungen**.

3. Klicken Sie im folgenden Fenster auf der Registerkarte **Allgemein** im Abschnitt **Schutzbereich** auf die Schaltfläche **Hinzufügen**.

4. Wählen Sie im Fenster **Untersuchungsobjekt** wählen ein Objekt aus und klicken Sie auf die Schaltfläche **Hinzufügen**. Nachdem alle erforderlichen Objekte hinzugefügt wurden, klicken Sie auf **OK**.

5. Um ein Objekt aus der Untersuchungsliste auszuschließen, deaktivieren Sie das entsprechende Kontrollkästchen.

➡ *Gehen Sie folgendermaßen vor, um den Typ der zu untersuchenden Dateien zu ändern:*

1. Öffnen Sie das Programmhauptfenster und klicken Sie im oberen Bereich des Fensters auf die Schaltfläche **Einstellungen**.

2. Klicken Sie im folgenden Fenster auf die Schaltfläche **Einstellungen**.

3. Wählen Sie im folgenden Fenster auf der Registerkarte **Allgemein** im Block **Dateitypen** den gewünschten Parameter.

HEURISTISCHE ANALYSE VERWENDEN

In der Grundeinstellung erfolgt die Untersuchung auf Basis der Datenbanken, die eine Beschreibung der bekannten Bedrohungen und entsprechende Desinfektionsmethoden enthalten. Kaspersky Anti-Virus vergleicht ein gefundenes Objekt mit den Einträgen in den Datenbanken, wodurch Sie eine eindeutige Antwort darauf erhalten, ob das untersuchte Objekt schädlich ist und zu welcher Klasse der gefährlichen Programme es gehört. Dieses Vorgehen wird als *Signaturanalyse* bezeichnet und wird standardmäßig verwendet.

Allerdings tauchen jeden Tag neue schädliche Objekte auf, die noch nicht in die Datenbanken aufgenommen wurden. Bei der Erkennung solcher Objekte hilft die heuristische Analyse. Diese Methode umfasst die Analyse der Aktivität, die ein Objekt im System zeigt. Wenn die erkannte Aktivität als typisch für schädliche Objekte gilt, lässt sich ein Objekt mit hoher Wahrscheinlichkeit als schädlich oder verdächtig einstufen. Dadurch können neue Bedrohungen bereits erkannt werden, bevor die Virenanalytiker von ihrer Aktivität wissen.

Zusätzlich können Sie das Genauigkeitsniveau der Untersuchung festlegen. Diese Einstellung reguliert das Verhältnis zwischen Ausführlichkeit der Suche, Auslastungsniveau der Betriebssystemressourcen und Untersuchungsdauer. Je höher das für die Untersuchung gewählte Niveau, desto mehr Systemressourcen sind dafür erforderlich und desto mehr Zeit wird beansprucht.

➡ *Gehen Sie folgendermaßen vor, um die heuristische Analyse zu verwenden und die Untersuchungsgenauigkeit festzulegen:*

1. Öffnen Sie das Programmhauptfenster und klicken Sie im oberen Bereich des Fensters auf die Schaltfläche **Einstellungen**.

2. Wählen Sie im folgenden Fenster die Komponente **Datei-Anti-Virus** und klicken Sie auf die Schaltfläche **Einstellungen**.

3. Aktivieren Sie im folgenden Fenster auf der Registerkarte **Leistung** im Block **Untersuchungsmethoden** das Kontrollkästchen ☑ **Heuristische Analyse** und stellen Sie darunter die Genauigkeitsstufe der Untersuchung ein.

OPTIMIERUNG DER UNTERSUCHUNG

Um die Untersuchungsdauer zu reduzieren und die Arbeitsgeschwindigkeit von Kaspersky Anti-Virus zu steigern, können Sie festlegen, dass nur neue Dateien und Dateien, die seit ihrer letzten Analyse verändert wurden, untersucht werden. Dieser Modus erstreckt sich auf gewöhnliche und zusammengesetzte Dateien.

➡ *Gehen Sie folgendermaßen vor, damit nur neue Dateien und Dateien, die seit der letzten Analyse verändert wurden, untersucht werden:*

1. Öffnen Sie das Programmhauptfenster und klicken Sie im oberen Bereich des Fensters auf die Schaltfläche **Einstellungen**.

2. Wählen Sie im folgenden Fenster die Komponente **Datei-Anti-Virus** und klicken Sie auf die Schaltfläche **Einstellungen**.

3. Aktivieren Sie im folgenden Fenster auf der Registerkarte **Leistung** das Kontrollkästchen ☑ **Nur neue und veränderte Dateien untersuchen**.

UNTERSUCHUNG VON ZUSAMMENGESETZTEN DATEIEN

Eine häufige Methode zum Verstecken von Viren ist das Eindringen von Schädlingen in zusammengesetzte Dateien wie Archive, Datenbanken usw. Um Viren zu erkennen, die auf diese Weise versteckt wurden, muss eine zusammengesetzte Datei entpackt werden. Dadurch kann das Untersuchungstempo wesentlich sinken.

Installationspakete und Dateien, die OLE-Objekte enthalten, werden beim Öffnen ausgeführt und gelten deshalb als gefährlicher als Archive. Wenn Sie die Untersuchung von Archiven deaktivieren und die Untersuchung von Dateien dieser Typen aktivieren, schützen Sie Ihren Computer vor der Ausführung von schädlichem Code und steigern gleichzeitig die Untersuchungsgeschwindigkeit.

Wenn eine Datei, die ein OLE-Objekt enthält, ein Archiv darstellt, wird sie beim Entpacken untersucht. Sie können die Untersuchung der Archive aktivieren, um die Dateien mit OLE-Objekten zu untersuchen, die sich in einem Archive befinden, vor seinem Entpacken. Allerdings sinkt das Untersuchungstempo wesentlich.

In der Grundeinstellung untersucht Kaspersky Anti-Virus nur angehängte OLE-Objekte.

Gehen Sie folgendermaßen vor, um Liste der zu untersuchenden zusammengesetzten Dateien zu ändern:

1. Öffnen Sie das Programmhauptfenster und klicken Sie im oberen Bereich des Fensters auf die Schaltfläche **Einstellungen**.
2. Wählen Sie im folgenden Fenster die Komponente **Datei-Anti-Virus** und klicken Sie auf die Schaltfläche **Einstellungen**.
3. Aktivieren Sie im folgenden Fenster auf der Registerkarte **Leistung** im Block **Untersuchung von zusammengesetzten Dateien** die Kontrollkästchen der zusammengesetzten Dateien, die von der Anwendung untersucht werden sollen.

UNTERSUCHUNG UMFANGREICHER ZUSAMMENGESETZTER DATEIEN

Bei der Untersuchung von umfangreichen zusammengesetzten Dateien kann das vorausgehende Entpacken viel Zeit beanspruchen. Die Zeit kann reduziert werden, wenn die Untersuchung von Dateien im Hintergrundmodus erfolgt. Wenn bei der Arbeit mit einer solchen Datei ein schädliches Objekt gefunden wird, werden Sie von Kaspersky Anti-Virus darüber informiert.

Die Verzögerung beim Zugriff auf zusammengesetzte Dateien lässt sich reduzieren, indem das Entpacken von Dateien, die eine bestimmte Größe überschreiten, ausgeschaltet wird. Beim Extrahieren aus Archiven werden Dateien immer untersucht.

Gehen Sie folgendermaßen vor, damit die Anwendung große Dateien im Hintergrundmodus entpackt:

1. Öffnen Sie das Programmhauptfenster und klicken Sie im oberen Bereich des Fensters auf die Schaltfläche **Einstellungen**.
2. Wählen Sie im folgenden Fenster die Komponente **Datei-Anti-Virus** und klicken Sie auf die Schaltfläche **Einstellungen**.
3. Klicken Sie im folgenden Fenster auf der Registerkarte **Leistung** im Block **Untersuchung von zusammengesetzten Dateien** auf die Schaltfläche **Erweitert**.
4. Aktivieren Sie im Fenster **Zusammengesetzte Dateien** das Kontrollkästchen **Zusammengesetzte Dateien im Hintergrund entpacken** und legen Sie im Feld unten einen Wert für die minimale Dateigröße fest.

Gehen Sie folgendermaßen vor, damit die Anwendung große zusammengesetzte Dateien nicht entpackt:

1. Öffnen Sie das Programmhauptfenster und klicken Sie im oberen Bereich des Fensters auf die Schaltfläche **Einstellungen**.
2. Wählen Sie im folgenden Fenster die Komponente **Datei-Anti-Virus** und klicken Sie auf die Schaltfläche **Einstellungen**.
3. Klicken Sie im folgenden Fenster auf der Registerkarte **Leistung** im Block **Untersuchung von zusammengesetzten Dateien** auf die Schaltfläche **Erweitert**.

4. Aktivieren Sie im Fenster **Zusammengesetzte Dateien** das Kontrollkästchen ☑ **Große zusammengesetzte Dateien nicht entpacken** und legen Sie im Feld unten einen Wert für die maximale Dateigröße fest.

UNTERSUCHUNGSMODUS ÄNDERN

Unter Untersuchungsmodus wird die Bedingung für das Auslösen von Datei-Anti-Virus verstanden. In der Grundeinstellung verwendet das Programm den intelligenten Modus, in dem die Entscheidung über die Untersuchung eines Objekts auf Basis der Operationen, die damit ausgeführt werden sollen, gefällt wird. Bei der Arbeit mit einem Microsoft Office-Dokument untersucht die Anwendung die Datei, wenn sie zum ersten Mal geöffnet und zum letzten Mal geschlossen wird. Alle dazwischen liegenden Operationen, bei denen die Datei verändert wird, werden von der Untersuchung ausgeschlossen.

Sie können den Untersuchungsmodus für Objekte ändern. Der passende Modus ist davon abhängig, mit welcher Art von Dateien Sie überwiegend arbeiten.

➡ *Gehen Sie folgendermaßen vor, um den Untersuchungsmodus für Objekte zu ändern:*

1. Öffnen Sie das Programmhauptfenster und klicken Sie im oberen Bereich des Fensters auf die Schaltfläche **Einstellungen**.

2. Wählen Sie im folgenden Fenster die Komponente **Datei-Anti-Virus** und klicken Sie auf die Schaltfläche **Einstellungen**.

3. Wählen Sie im folgenden Fenster auf der Registerkarte **Erweitert** im Block **Untersuchungsmodus** den erforderlichen Modus.

UNTERSUCHUNGSTECHNOLOGIE

Zusätzlich können Sie eine Technologie wählen, die von Datei-Anti-Virus verwendet werden soll:

- **iChecker**. Eine Technologie, die eine Steigerung der Untersuchungsgeschwindigkeit erlaubt, indem bestimmte Objekte ausgeschlossen werden. Dabei wird ein Objekt nach einem speziellen Algorithmus von der Untersuchung ausgeschlossen, der das Erscheinungsdatum der Programm-Datenbanken, das Datum der letzten Untersuchung des Objekts und die Änderung von Untersuchungsparametern berücksichtigt.

  Es kann beispielsweise sein, dass einer Archivdatei aufgrund der Untersuchungsergebnisse der Status *virenfrei* zugewiesen wurde. Dann wird das Archiv von der folgenden Untersuchung ausgeschlossen, wenn es nicht verändert wurde und die Untersuchungsparameter gleich geblieben sind. Wenn seit der letzten Untersuchung die Zusammensetzung des Archivs durch Hinzufügen eines neuen Objekts verändert wurde, die Untersuchungsparameter geändert oder die Programm-Datenbanken aktualisiert wurden, wird das Archiv erneut untersucht.

  Die Technologie iChecker besitzt folgende Einschränkungen: Sie funktioniert nicht mit umfangreichen Dateien und kann nur auf Objekte angewandt werden, deren Struktur dem Programm bekannt ist (z.B. die Dateiformate exe, dll, lnk, ttf, inf, sys, com, chm, zip, rar).

- **iSwift**. Diese Technologie stellt eine Weiterentwicklung der iChecker-Technologie für Computer mit NTFS-Dateisystem dar. Die Technologie iSwift besitzt folgende Einschränkungen: Sie ist an einen konkreten Ort der Datei im Dateisystem gebunden und kann nur auf Objekte angewandt werden, die sich in einem NTFS-Dateisystem befinden.

➡ *Gehen Sie folgendermaßen vor, um die Untersuchungstechnologie für Objekte zu ändern:*

1. Öffnen Sie das Programmhauptfenster und klicken Sie im oberen Bereich des Fensters auf die Schaltfläche **Einstellungen**.

2. Wählen Sie im folgenden Fenster die Komponente **Datei-Anti-Virus** und klicken Sie auf die Schaltfläche **Einstellungen**.

3. Wählen Sie im folgenden Fenster auf der Registerkarte **Erweitert** im Block **Untersuchungstechnologien** den erforderlichen Parameterwert.

KOMPONENTE ANHALTEN: ZEITPLAN ERSTELLEN

Bei der Ausführung von Arbeiten, die die Betriebssystemressourcen stark beanspruchen, können Sie die Arbeit von Datei-Anti-Virus vorübergehend anhalten. Um die Belastung zu verringern und den schnellen Zugriff auf Objekte zu gewährleisten, kann in den Einstellungen festlegt werden, dass die Komponente für einen bestimmten Zeitraum angehalten wird.

Gehen Sie folgendermaßen vor, um den Zeitplan anzupassen, nach dem eine Komponente angehalten werden soll:

1. Öffnen Sie das Programmhauptfenster und klicken Sie im oberen Bereich des Fensters auf die Schaltfläche **Einstellungen**.

2. Wählen Sie im folgenden Fenster die Komponente **Datei-Anti-Virus** und klicken Sie auf die Schaltfläche **Einstellungen**.

3. Aktivieren Sie im folgenden Fenster auf der Registerkarte **Erweitert** im Block **Aufgabe anhalten** das Kontrollkästchen ☑ **Nach Zeitplan** und klicken Sie auf die Schaltfläche **Zeitplan**.

4. Legen Sie im Fenster **Aufgabe anhalten** (in den Feldern **Anhalten um** und **Fortsetzen um**) den Zeitraum fest, für den der Schutz angehalten werden soll (im Format HH:MM).

KOMPONENTE ANHALTEN: LISTE DER PROGRAMME ERSTELLEN

Bei der Ausführung von Arbeiten, die die Betriebssystemressourcen stark beanspruchen, können Sie die Arbeit von Datei-Anti-Virus vorübergehend anhalten. Um die Belastung zu verringern und den schnellen Zugriff auf Objekte zu gewährleisten, kann in den Einstellungen festlegt werden, dass die Komponente bei der Arbeit mit bestimmten Programmen angehalten wird.

Das Deaktivieren von Datei-Anti-Virus bei einem Konflikt mit bestimmten Programmen gilt als Notlösung! Sollten bei der Arbeit von Datei-Anti-Virus Konflikte auftreten, dann wenden Sie sich an den Technischen Support von Kaspersky Lab (http://support.kaspersky.de). Die Support-Spezialisten helfen Ihnen dabei, die gemeinsame Arbeit von Kaspersky Anti-Virus mit anderen Anwendungen auf dem Computer einzurichten.

Gehen Sie folgendermaßen vor, um festzulegen, dass die Komponente angehalten wird, während die angegebenen Programme arbeiten:

1. Öffnen Sie das Programmhauptfenster und klicken Sie im oberen Bereich des Fensters auf die Schaltfläche **Einstellungen**.

2. Wählen Sie im folgenden Fenster die Komponente **Datei-Anti-Virus** und klicken Sie auf die Schaltfläche **Einstellungen**.

3. Aktivieren Sie im folgenden Fenster auf der Registerkarte **Erweitert** im Block **Aufgabe anhalten** das Kontrollkästchen ☑ **Beim Start bestimmter Anwendungen** und klicken Sie auf die Schaltfläche **Wählen**.

4. Legen Sie im Fenster **Programme** die Liste der Programme an, bei deren Arbeit die Komponente angehalten werden soll.

STANDARDMÄßIGE SCHUTZPARAMETER WIEDERHERSTELLEN

Während Sie die Arbeit von Datei-Anti-Virus konfigurieren, können Sie jederzeit zu den empfohlenen Einstellungen zurückkehren. Diese gelten als optimal, werden von den Kaspersky-Lab-Spezialisten empfohlen und sind in der Sicherheitsstufe **Empfohlen** zusammengefasst.

Wenn Sie bei der Konfiguration von Datei-Anti-Virus die Liste der Objekte verändert haben, die zum Schutzbereich gehören, dann wird Ihnen beim Wiederherstellen der ursprünglichen Einstellungen vorgeschlagen, diese Liste zur späteren Verwendung zu speichern.

➡ *Gehen Sie folgendermaßen vor, um die standardmäßigen Schutzeinstellungen wiederherzustellen und eine geänderte Liste der Objekte, die dem Schutzbereich angehören, zu speichern:*

1. Öffnen Sie das Programmhauptfenster und klicken Sie im oberen Bereich des Fensters auf die Schaltfläche **Einstellungen**.

2. Wählen Sie im folgenden Fenster die Komponente **Datei-Anti-Virus** und klicken Sie auf die Schaltfläche **Grundeinstellung**.

3. Aktivieren Sie im folgenden Fenster **Einstellungen wiederherstellen** das Kontrollkästchen ☑ **Schutzbereich**.

STATISTIK ÜBER DEN DATEISCHUTZ

Alle von Datei-Anti-Virus ausgeführten Operationen werden in einem speziellen Bericht aufgezeichnet. Verwenden Sie den Link **Statistik**, um Informationen über die Arbeit der Komponente zu erhalten. Dadurch wird ein detaillierter Bericht über die Arbeit der Komponente geöffnet, der aus folgenden Registerkarten besteht:

- Alle gefährlichen Objekte, die beim Schutz des Dateisystems gefunden wurden, werden auf der Registerkarte *Gefunden* aufgezählt. Hier wird der vollständige Pfad des Fundorts für jedes Objekt und der Status, den Datei-Anti-Virus dem Objekt verliehen hat, genannt: wenn genau ermittelt werden konnte, von welchem Schadprogramm das Objekt infiziert ist, erhält es den entsprechenden Status (z.B. Virus, trojanisches Programm usw.). Wenn sich der Malware-Typ nicht genau feststellen lässt, erhält das Objekt den Status *verdächtig*. Neben dem Status wird außerdem die Aktion genannt, die mit dem Objekt ausgeführt wurde (gefunden, nicht gefunden, desinfiziert).

  Damit auf dieser Registerkarte keine Informationen über desinfizierte Objekte angezeigt werden, deaktivieren Sie das Kontrollkästchen ☑ **Desinfizierte Objekte anzeigen**.

- Eine vollständige Liste der Ereignisse, die bei der Arbeit von Datei-Anti-Virus eingetreten sind, befindet sich auf der Registerkarte *Ereignisse*. Die Ereignisse können folgende Status besitzen:

  - *Informatives Ereignis* (z.B.: Objekt wurde nicht verarbeitet: nach Typ übersprungen).
  - *Warnung* (z.B.: Virus gefunden).
  - *Hinweis* (z.B.: Archiv ist kennwortgeschützt).

  In der Regel besitzen informative Ereignisse begleitenden Charakter und sind nebensächlich. Sie können die Anzeige von informativen Meldungen abschalten. Deaktivieren Sie dazu das Kontrollkästchen ☑ **Alle Ereignisse anzeigen**.

- Die Untersuchungsstatistik befindet sich auf der Registerkarte *Statistik*. Hier wird die Gesamtzahl der untersuchten Objekte genannt. In speziellen Spalten wird darüber informiert, wie viele Archive und gefährliche Objekte sich unter den untersuchten Objekte befanden, wie viele Objekte desinfiziert, in die Quarantäne verschoben wurden, usw.

- Die *Einstellungen*, mit denen der Datei-Anti-Virus arbeitet, befinden sich auf der gleichnamigen Registerkarte. Verwenden Sie den Link **Einstellungen ändern**, um schnell zur Konfiguration der Komponente zu gelangen.

- Die Registerkarte *Blockierte Benutzer* enthält eine Liste der Benutzer, deren Computer bei dem Versuch gesperrt wurden, ein infiziertes oder möglicherweise infiziertes Objekt auf den Server zu kopieren.

AUFGESCHOBENE DESINFEKTION VON OBJEKTEN

In Kaspersky Anti-Virus für Windows Server MP4 wird der Zugriff auf infizierte Objekte gesperrt, wenn die Desinfektion fehlschlägt oder wenn das Objekt gelöscht wird.

Um erneut Zugriff auf blockierte Objekte zu erhalten, muss vorher ein Desinfektionsversuch ausgeführt werden. Wenn die Desinfektion des Objekts gelingt, wird der Zugriff darauf freigegeben. Kann das Objekt nicht desinfiziert werden, dann wird Ihnen zur Auswahl angeboten, es zu *löschen* oder zu *überspringen*. Beim Überspringen wird die Datei für den Zugriff freigegeben. Allerdings erhöht sich dadurch das Risiko einer Infektion des Servers erheblich. Es wird ausdrücklich davor gewarnt, schädliche Objekte zu überspringen.

➡ *Gehen Sie folgendermaßen vor, um Zugriff auf blockierte Objekte zu erhalten, wenn Sie diese desinfizieren möchten:*

1. Öffnen Sie das Programmhauptfenster und klicken Sie auf die Schaltfläche **Gefunden**

2. Wählen Sie im folgenden Fenster auf der Registerkarte **Aktive Bedrohungen** die erforderlichen Objekte aus und klicken Sie auf den Link **Alle desinfizieren**.

SIEHE AUCH

Aktion für gefundene Objekte ändern 41

UNTERSUCHUNG DES SERVERS AUF VIREN

Kaspersky Anti-Virus 6.0 für Windows Server MP4 erlaubt es, sowohl einzelne Objekte (Dateien, Ordner, Laufwerke, Wechseldatenträger) als auch den gesamten Server auf das Vorhandensein von Viren zu untersuchen. Durch die Virensuche lässt sich die Möglichkeit der Ausbreitung eines schädlichen Codes verhindern, der von Datei-Anti-Virus aus bestimmten Gründen nicht erkannt wurde.

Kaspersky Anti-Virus 6.0 für Windows Server MP4 verfügt über folgende standardmäßigen Untersuchungsaufgaben:

Virensuche

Untersuchung von Objekten, die der Benutzer festlegt. Sie können ein beliebiges Objekt des Dateisystems auf dem Computer untersuchen.

Vollständige Suche

Ausführliche Untersuchung des Systems. Standardmäßig werden folgende Objekte untersucht: Systemspeicher, Objekte, die beim Systemstart gestartet werden, Systemwiederherstellung, Mail-Datenbanken, Festplatten, Wechseldatenträger und Netzlaufwerke.

Schnelle Suche

Virenuntersuchung der Objekte, die beim Start des Betriebssystems geladen werden.

Diese Aufgaben werden standardmäßig mit den empfohlenen Einstellungen ausgeführt. Sie können diese Einstellungen ändern und einen Zeitplan für den Aufgabenstart festlegen.

Daneben können Sie ein beliebiges Objekt auf Viren untersuchen, ohne dafür eine spezielle Untersuchungsaufgabe zu erstellen. Das zu untersuchende Objekt kann aus dem Interface von Kaspersky Anti-Virus oder mit den Standardmitteln des Betriebssystems Microsoft Windows Server (beispielsweise im Fenster des Programms **Explorer** oder auf dem **Arbeitsplatz** usw.) ausgewählt werden. Führen Sie dazu den Mauszeiger auf den Namen des gewünschten Objekts, öffnen Sie mit der rechten Maustaste das Microsoft Windows-Kontextmenü und wählen Sie den Punkt **Auf Viren untersuchen**.

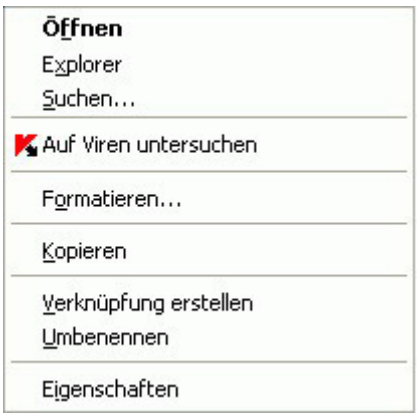


Abbildung 7. Kontextmenü von Microsoft Windows

Außerdem können Sie zum Bericht über die Untersuchung wechseln, der vollständige Informationen über die Ereignisse, die bei der Ausführung von Aufgaben eingetreten sind, bietet.

Gehen Sie folgendermaßen vor, um die Parameter einer bestimmten Untersuchungsaufgabe zu ändern:

1. Öffnen Sie das Programmhauptfenster.
2. Wählen Sie auf der linken Fensterseite den Abschnitt **Virensuche** (**Vollständige Suche**, **Schnelle Suche**).

3. Klicken Sie für den ausgewählten Abschnitt auf den Link mit der festgelegten Sicherheitsstufe.

4. Nehmen Sie im folgenden Fenster in den Einstellungen der gewählten Aufgabe die erforderlichen Änderungen vor.

Gehen Sie folgendermaßen vor, um einen Bericht über die Virenuntersuchung zu öffnen:

1. Öffnen Sie das Programmhauptfenster.

2. Wählen Sie auf der linken Fensterseite den Abschnitt **Virensuche** (**Vollständige Suche**, **Schnelle Suche**).

3. Klicken Sie auf die Schaltfläche **Berichte**.

IN DIESEM ABSCHNITT

START DER VIRENSUCHE

Die Virensuche lässt sich auf zwei Arten starten:

- aus dem Kontextmenü von Kaspersky Anti-Virus
- aus dem Hauptfenster von Kaspersky Anti-Virus

Informationen über den Verlauf der Aufgabenausführung werden im Hauptfenster von Kaspersky Anti-Virus angezeigt.

Außerdem können Sie ein Untersuchungsobjekt mit den Standardmitteln des Betriebssystems Microsoft Windows (beispielsweise im Fenster des Programms **Explorer** oder auf dem **Arbeitsplatz** usw.) auswählen.

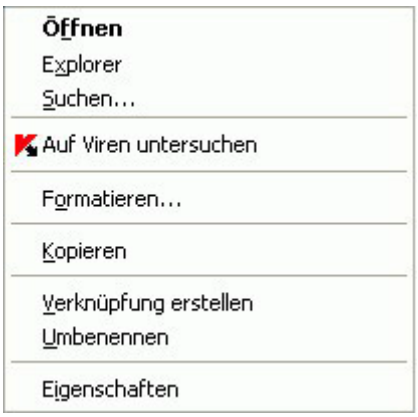


Abbildung 8. Kontextmenü von Microsoft Windows

- *Gehen Sie folgendermaßen vor, um eine Aufgabe zur Virensuche aus dem Kontextmenü zu starten:*

  1. Klicken Sie im Infobereich der Taskleiste mit der rechten Maustaste auf das Programmsymbol.
  2. Wählen sie im Kontextmenü den Punkt **Untersuchung** aus. Wählen Sie im Hauptfenster von Kaspersky Anti-Virus die Aufgabe **Virensuche** (**Vollständige Suche**, **Schnelle Suche**). Passen Sie bei Bedarf die Parameter der gewählten Aufgabe an und klicken Sie auf die Schaltfläche **Virensuche ausführen**.
  3. Oder wählen Sie im Kontextmenü den Punkt V**ollständige Suche**. Die vollständige Untersuchung des Computers wird gestartet. Der Verlauf der Aufgabenausführung wird im Hauptfenster von Kaspersky Anti-Virus dargestellt.

- *Gehen Sie folgendermaßen vor, um eine Aufgabe zur Virensuche aus dem Programmhauptfenster zu starten:*

  1. Öffnen Sie das Programmhauptfenster.
  2. Wählen Sie auf der linken Fensterseite den Abschnitt **Virensuche** (**Vollständige Suche**, **Schnelle Suche**).
  3. Klicken Sie für den ausgewählten Abschnitt auf die Schaltfläche **Virensuche ausführen**. Der Ausführungsfortschritt der Aufgabe wird im Programmhauptfenster dargestellt.

- *Gehen Sie folgendermaßen vor, um eine Aufgabe zur Virensuche für eine ausgewähltes Objekt aus dem Kontextmenü von Microsoft Windows zu starten:*

  1. Klicken Sie mit der rechten Maustaste auf den Namen des gewählten Objekts.
  2. Wählen Sie im Kontextmenü den Punkt **Auf Viren untersuchen**. Der Fortschritt und das Ergebnis der Aufgabenausführung werden im Statistikfenster dargestellt.

ERSTELLEN EINER LISTE DER UNTERSUCHUNGSOBJEKTE

Standardmäßig entspricht jeder Aufgabe zur Virensuche eine eigene Liste von Objekten. Um diese Liste anzuzeigen, wählen Sie im Abschnitt **Virensuche** des Programmhauptfensters den Namen einer Aufgabe (z.B. **Vollständige Suche**). Die Liste der Objekte wird auf der rechten Fensterseite angezeigt.

Für Aufgaben, die standardmäßig bei der Programminstallation erstellt wurden, besteht bereits eine Liste der zu untersuchenden Objekte.

Aus Gründen der Bedienungsfreundlichkeit können dem Untersuchungsbereich solche Kategorien wie Posteingänge des Benutzers, Systemspeicher, Autostart-Objekte, Sicherungsdateien des Betriebssystems und Objekte, die sich im Quarantäneordner von Kaspersky Anti-Virus befinden, hinzugefügt werden.

Außerdem kann beim Hinzufügen eines Ordners, der untergeordnete Objekte enthält, die rekursive Untersuchung geändert werden. Wählen Sie dazu das Objekt in der Liste der Untersuchungsobjekte aus, öffnen Sie das Kontextmenü und verwenden Sie den Befehl **Unterordner einschließen**.

Gehen Sie folgendermaßen vor, um eine Liste der Untersuchungsobjekte zu erstellen:

1. Öffnen Sie das Programmhauptfenster.
2. Wählen Sie auf der linken Fensterseite den Abschnitt **Virensuche** (**Vollständige Suche**, **Schnelle Suche**).
3. Klicken Sie im ausgewählten Abschnitt auf den Link **Hinzufügen**.
4. Wählen Sie im folgenden Fenster **Untersuchungsobjekt** wählen ein Objekt aus und klicken Sie auf die Schaltfläche **Hinzufügen**. Nachdem alle erforderlichen Objekte hinzugefügt wurden, klicken Sie auf **OK**. Um bestimmte Objekte von der Untersuchung auszuschließen, deaktivieren Sie in der Liste das entsprechende Kontrollkästchen. Um ein Objekt aus der Liste zu entfernen, markieren Sie es und verwenden Sie den Link **Löschen**.

ÄNDERN DER SICHERHEITSSTUFE

Unter Sicherheitsstufe wird eine vordefinierte Auswahl von Untersuchungsparametern verstanden. Die Spezialisten von Kaspersky Lab haben drei Sicherheitsstufen vordefiniert. Die Auswahl der Sicherheitsstufe können Sie je nach persönlichen Präferenzen selbst treffen:

- Wenn Sie das Infektionsrisiko für Ihren Computer sehr hoch einschätzen, wählen Sie die hohe Sicherheitsstufe.
- Die empfohlene Stufe ist in den meisten Fälle geeignet und wird von den Kaspersky-Lab-Spezialisten empfohlen.
- Wenn Sie mit Programmen arbeiten, die den Arbeitsspeicher stark beanspruchen, wählen Sie die niedrige Sicherheitsstufe, da die Auswahl der untersuchten Dateien auf dieser Stufe eingeschränkt wird.

Wenn keine der vordefinierten Stufen Ihren Anforderungen entspricht, können Sie die Untersuchungsparameter anpassen. Dadurch ändert sich der Name der Sicherheitsstufe in **Benutzerdefiniert**. Um die standardmäßigen Einstellungen der Komponente wiederherzustellen, wählen Sie eine der vordefinierten Stufen. Die Untersuchung erfolgt standardmäßig auf der **Empfohlenen** Stufe.

Gehen Sie folgendermaßen vor, um die festgelegte Sicherheitsstufe zu ändern:

1. Öffnen Sie das Programmhauptfenster.
2. Wählen Sie auf der linken Fensterseite den Abschnitt **Virensuche** (**Vollständige Suche**, **Schnelle Suche**).
3. Klicken Sie für den ausgewählten Abschnitt auf den Link mit der festgelegten Sicherheitsstufe.
4. Verschieben Sie im folgenden Fenster im Block **Sicherheitsstufe** den Zeiger auf der Skala. Durch das Anpassen der Sicherheitsstufe wird das Verhältnis zwischen der Ausführungsgeschwindigkeit der Untersuchung und der Anzahl der zu untersuchenden Dateien bestimmt: je weniger Dateien der Virenanalyse unterzogen werden, desto höher ist die Untersuchungsgeschwindigkeit. Oder klicken Sie auf die Schaltfläche **Einstellungen** und wählen Sie im folgenden Fenster die erforderlichen Parameter aus. Die Sicherheitsstufe ändert sich in **Benutzerdefiniert**.

ÄNDERN DER AKTION BEIM FUND EINER BEDROHUNG

Wenn sich durch die Virenuntersuchung eines Objekts herausstellt, dass es infiziert oder verdächtig ist, hängen die weiteren Operationen des Programms vom Status des Objekts und von der ausgewählten Aktion ab.

Ein Objekt kann aufgrund der Untersuchung einen der folgenden Status erhalten:

- Status eines der schädlichen Programme (beispielsweise *Virus*, *trojanisches Programm*).
- *möglicherweise infiziert*, wenn sich aufgrund der Untersuchung nicht eindeutig feststellen lässt, ob das Objekt infiziert ist oder nicht. Möglicherweise wurde in der Datei der Codes eines unbekannten Virus oder der modifizierte Code eines bekannten Virus gefunden.

Standardmäßig werden alle infizierten Dateien der Desinfektion unterzogen und alle möglicherweise infizierten Dateien in die Quarantäne verschoben.

GEWÄHLTE AKTION	WAS GESCHIEHT BEIM FUND EINES INFIZIERTEN / MÖGLICHERWEISE INFIZIERTEN OBJEKTS?
◉ **Nach Abschluss der Untersuchung erfragen**	Das Programm schiebt die Verarbeitung von Objekten bis zum Abschluss der Untersuchung auf. Nach dem Abschluss der Untersuchung erscheint nacheinander für jedes Objekt eine Aktionsanfrage.
◉ **Während der Untersuchung erfragen**	Das Programm zeigt eine Warnmeldung auf dem Bildschirm an, die darüber informiert, von welchem schädlichen Code das Objekt infiziert / möglicherweise infiziert ist, und bietet Aktionen zur Auswahl an.
◉ **Nicht erfragen**	Das Programm protokolliert im Bericht Informationen über die gefundenen Objekte. Es wird davor gewarnt, diesen Funktionsmodus für das Programm zu wählen, weil infizierte und möglicherweise infizierte Objekte dann auf Ihrem Computer verbleiben und es praktisch unmöglich ist, eine Infektion zu verhindern.
◉ **Nicht erfragen** ☑ **Desinfizieren**	Das Programm protokolliert im Bericht Informationen über die gefundenen Objekte. Die Objekte werden nicht verarbeitet und es erfolgt keine Meldung. Es wird davor gewarnt, diesen Funktionsmodus für das Programm zu wählen, weil infizierte und möglicherweise infizierte Objekte dann auf dem Server verbleiben und es praktisch unmöglich ist, eine Infektion zu verhindern.
◉ **Nicht erfragen** ☑ **Desinfizieren** ☑ **Löschen, wenn Desinfektion nicht möglich**	Das Programm führt einen Desinfektionsversuch mit dem gefundenen Objekt aus, ohne nach der Bestätigung des Benutzers zu fragen. Wenn der Desinfektionsversuch fehlschlägt, wird es gelöscht. Eine Kopie des Objekts wird im Backup-Speicher abgelegt.
◉ **Nicht erfragen** ☐ **Desinfizieren** ☑ **Löschen**	Das Programm löscht das Objekt automatisch.

Bevor ein Desinfektionsversuch erfolgt oder ein Objekt gelöscht wird, legt Kaspersky Anti-Virus eine Sicherungskopie des Objekts an und speichert diese im Backup. Dadurch wird erlaubt, das Objekt bei Bedarf wiederherzustellen oder später zu desinfizieren.

Objekte mit dem Status *möglicherweise infiziert* werden ohne vorherigen Desinfektionsversuch in die Quarantäne verschoben.

➡ *Gehen Sie folgendermaßen vor, um die festgelegte Aktion für gefundene Objekte zu ändern:*

1. Öffnen Sie das Programmhauptfenster.
2. Wählen Sie auf der linken Fensterseite den Abschnitt **Virensuche** (**Vollständige Suche**, **Schnelle Suche**).
3. Klicken Sie für den ausgewählten Abschnitt auf den Link mit der festgelegten Sicherheitsstufe.
4. Nehmen Sie im folgenden Fenster im Block **Aktion** die erforderlichen Änderungen vor.

ÄNDERN DES TYPS DER ZU UNTERSUCHENDEN OBJEKTE

Durch die Angabe des Typs der zu untersuchenden Objekte bestimmen Sie das Format und die Größe der Dateien, die beim Ausführen der gewählten Aufgabe untersucht werden sollen.

Bei der Auswahl des Dateityps muss Folgendes beachtet werden:

- Für bestimmte Dateiformate ist das Risiko des Eindringens von schädlichem Code und der späteren Aktivierung relativ gering ist (z.B. *txt*). Gleichzeitig gibt es Formate, die ausführbaren Code enthalten oder enthalten können (*exe*, *dll*, *doc*). Das Risiko des Eindringens und der Aktivierung von schädlichem Code ist für solche Dateien relativ hoch.

- Es sollte beachtet werden, dass ein Angreifer einen Virus in einer Datei mit der Erweiterung *txt* an Ihren Computer senden kann, obwohl es sich in Wirklichkeit um eine ausführbare Datei handelt, die in eine *txt*-Datei umbenannt wurde. Wenn die Variante **Dateien nach Erweiterung untersuchen** gewählt wurde, wird eine solche Datei bei der Untersuchung übersprungen. Wenn Sie die Variante **Dateien nach Format untersuchen** gewählt haben, analysiert der Dateischutz ungeachtet der Erweiterung die Kopfzeile der Datei, wodurch sich ergibt, dass die Datei das Format exe besitzt. Eine solche Datei wird der sorgfältigen Virenuntersuchung unterzogen.

Gehen Sie folgendermaßen vor, um den Typ der zu untersuchenden Dateien zu ändern:

1. Öffnen Sie das Programmhauptfenster.
2. Wählen Sie auf der linken Fensterseite den Abschnitt **Virensuche** (**Vollständige Suche**, **Schnelle Suche**).
3. Klicken Sie für den ausgewählten Abschnitt auf den Link mit der festgelegten Sicherheitsstufe.
4. Klicken Sie im folgenden Fenster im Block **Sicherheitsstufe** auf die Schaltfläche **Einstellungen**.
5. Wählen Sie auf der Registerkarte **Gültigkeitsbereich** im Block **Dateitypen** den gewünschten Parameter.

OPTIMIERUNG DER UNTERSUCHUNG

Sie können die Untersuchungszeit verkürzen und die Arbeitsgeschwindigkeit von Kaspersky Anti-Virus erhöhen. Damit nur neue Dateien und Dateien, die seit der letzten Analyse verändert wurden, untersucht werden. Dieser Untersuchungsmodus erstreckt sich auf gewöhnliche und zusammengesetzte Dateien.

Außerdem kann die Untersuchungsdauer beschränkt werden. Nach Ablauf der festgelegten Zeit, wird die Dateiuntersuchung abgebrochen. Außerdem können Sie bestimmen, bis zu welcher maximalen Größe eine Datei untersucht werden soll. Wenn die Größe den festgelegten Wert überschreitet, wird die Datei von der Untersuchung ausgeschlossen.

Gehen Sie folgendermaßen vor, damit nur neue und veränderte Dateien untersucht werden:

1. Öffnen Sie das Programmhauptfenster.
2. Wählen Sie auf der linken Fensterseite den Abschnitt **Virensuche** (**Vollständige Suche**, **Schnelle Suche**).
3. Klicken Sie für den ausgewählten Abschnitt auf den Link mit der festgelegten Sicherheitsstufe.
4. Klicken Sie im folgenden Fenster im Block **Sicherheitsstufe** auf die Schaltfläche **Einstellungen**.
5. Aktivieren Sie im folgenden Fenster auf der Registerkarte **Gültigkeitsbereich** im Block **Optimierung der Untersuchung** das Kontrollkästchen **Nur neue und veränderte Dateien untersuchen**.

Gehen Sie folgendermaßen vor, um eine zeitliche Begrenzung für die Untersuchung festzulegen:

1. Öffnen Sie das Programmhauptfenster.

2. Wählen Sie auf der linken Fensterseite den Abschnitt **Virensuche** (**Vollständige Suche**, **Schnelle Suche**).

3. Klicken Sie für den ausgewählten Abschnitt auf den Link mit der festgelegten Sicherheitsstufe.

4. Klicken Sie im folgenden Fenster im Block **Sicherheitsstufe** auf die Schaltfläche **Einstellungen**.

5. Aktivieren Sie im folgenden Fenster auf der Registerkarte **Gültigkeitsbereich** im Block **Optimierung der Untersuchung** das Kontrollkästchen ☑ **Untersuchung beenden, wenn länger als** und geben Sie im Feld daneben die Untersuchungsdauer an.

➧ *Gehen Sie folgendermaßen vor, um die Größe einer zu untersuchenden Datei zu beschränken:*

1. Öffnen Sie das Programmhauptfenster.

2. Wählen Sie auf der linken Fensterseite den Abschnitt **Virensuche** (**Vollständige Suche**, **Schnelle Suche**).

3. Klicken Sie für den ausgewählten Abschnitt auf den Link mit der festgelegten Sicherheitsstufe.

4. Klicken Sie im folgenden Fenster im Block **Sicherheitsstufe** auf die Schaltfläche **Einstellungen**.

5. Klicken Sie im folgenden Fenster auf der Registerkarte .**Gültigkeitsbereich** auf die Schaltfläche **Erweitert**.

6. Aktivieren Sie im Fenster **Zusammengesetzte Dateien** das Kontrollkästchen ☑ **HGroße zusammengesetzte Dateien nicht entpacken** und legen Sie im Feld unten einen Wert für die maximale Dateigröße fest.

UNTERSUCHUNG VON ZUSAMMENGESETZTEN DATEIEN

Eine häufige Methode zum Verstecken von Viren ist das Eindringen von Schädlingen in zusammengesetzte Dateien wie Archive, Datenbanken usw. Um Viren zu erkennen, die auf diese Weise versteckt wurden, muss eine zusammengesetzte Datei entpackt werden. Dadurch kann das Untersuchungstempo wesentlich sinken.

Für jeden Typ einer zusammengesetzten Datei können Sie auswählen, ob alle oder nur neue Dateien untersucht werden sollen. Verwenden Sie dazu den Link neben dem Namen des Objekts. Der Link verändert seinen Wert, wenn mit der linken Maustaste darauf geklickt wird. Wenn festgelegt wurden, dass nur neue und veränderte Dateien untersucht werden sollen, ist die Auswahl des Typs für zusammengesetzte Dateien nicht verfügbar.

➧ *Gehen Sie folgendermaßen vor, um Liste der zu untersuchenden zusammengesetzten Dateien zu ändern:*

1. Öffnen Sie das Programmhauptfenster.

2. Wählen Sie auf der linken Fensterseite den Abschnitt **Virensuche** (**Vollständige Suche**, **Schnelle Suche**).

3. Klicken Sie für den ausgewählten Abschnitt auf den Link mit der festgelegten Sicherheitsstufe.

4. Klicken Sie im folgenden Fenster im Block **Sicherheitsstufe** auf die Schaltfläche **Einstellungen**.

5. Wählen Sie im folgenden Fenster auf der Registerkarte **Gültigkeitsbereich** im Block **Untersuchung von zusammengesetzten Dateien** den erforderlichen Typ für die zu untersuchenden zusammengesetzten Dateien.

UNTERSUCHUNGSMETHODE ÄNDERN

Sie können die *heuristische Analyse* zur Prüfung verwenden. Diese Methode besteht in der Analyse der Aktivität, die ein Objekt im System zeigt. Wenn die erkannte Aktivität als typisch für schädliche Objekte gilt, lässt sich ein Objekt mit hoher Wahrscheinlichkeit als schädlich oder verdächtig einstufen.

Zusätzlich können Sie die Genauigkeitsstufe der Untersuchung anpassen. Bewegen Sie dazu den Schieberegler auf die gewünschte Position: **oberflächlich**, **mittel** oder **tief**.

Neben diesen Untersuchungsmethoden steht noch die Rootkit-Suche zur Verfügung. Ein *Rootkit* ist eine Kombination von Utilities, die schädliche Programme im Betriebssystem verstecken. Solche Tools dringen in das System ein. Sie tarnen ihre eigene Existenz und verstecken im System die Prozesse, Ordner oder Registrierungsschlüssel anderer Malware, die in der Konfiguration des Rootkits beschrieben ist. Wenn die Rootkit-Suche aktiviert ist, können Sie die Detailstufe für die Suche nach Rootkits wählen (Erweiterte Analyse). In diesem Fall wird die ausführliche Suche nach solchen Programmen ausgeführt, wobei eine große Anzahl von Objekten unterschiedlicher Typen analysiert wird.

Gehen Sie folgendermaßen vor, um die erforderlichen Untersuchungsmethoden zu verwenden:

1. Öffnen Sie das Programmhauptfenster.
2. Wählen Sie auf der linken Fensterseite den Abschnitt **Virensuche** (**Vollständige Suche**, **Schnelle Suche**).
3. Klicken Sie für den ausgewählten Abschnitt auf den Link mit der festgelegten Sicherheitsstufe.
4. Klicken Sie im folgenden Fenster im Block **Sicherheitsstufe** auf die Schaltfläche **Einstellungen**.
5. Wählen Sie im folgenden Fenster auf der Registerkarte **Erweitert** im Block **Untersuchungsmethoden** die erforderlichen Untersuchungsmethoden.

UNTERSUCHUNGSTECHNOLOGIE

Zusätzlich können Sie eine Technologie wählen, die bei der Untersuchung verwendet werden soll:

- **iChecker**. Eine Technologie, die eine Steigerung der Untersuchungsgeschwindigkeit erlaubt, indem bestimmte Objekte ausgeschlossen werden. Dabei wird ein Objekt nach einem speziellen Algorithmus von der Untersuchung ausgeschlossen, der das Erscheinungsdatum der Programm-Datenbanken, das Datum der letzten Untersuchung des Objekts und die Änderung von Untersuchungsparametern berücksichtigt.

  Eine Archivdatei wurde beispielsweise von Kaspersky Anti-Virus untersucht und ihr wurde der Status *virenfrei* zugewiesen. Dann wird das Archiv von der folgenden Untersuchung ausgeschlossen, wenn es nicht verändert wurde und die Untersuchungsparameter gleich geblieben sind. Wenn seit der letzten Untersuchung die Zusammensetzung des Archivs durch Hinzufügen eines neuen Objekts verändert wurde, die Untersuchungsparameter geändert oder die Programm-Datenbanken aktualisiert wurden, wird das Archiv erneut untersucht.

  Die Technologie iChecker besitzt folgende Einschränkungen: Sie funktioniert nicht mit großen Dateien und kann nur auf Objekte angewandt werden, deren Struktur dem Programm bekannt ist (z.B. die Dateiformate exe, dll, lnk, ttf, inf, sys, com, chm, zip, rar).

- **iSwift**. Diese Technologie stellt eine Weiterentwicklung der iChecker-Technologie für Computer mit NTFS-Dateisystem dar. Die Technologie iSwift besitzt folgende Einschränkungen: Sie ist an einen konkreten Ort der Datei im Dateisystem gebunden und kann nur auf Objekte angewandt werden, die sich in einem NTFS-Dateisystem befinden.

Gehen Sie folgendermaßen vor, um eine Untersuchungstechnologie für Objekte zu verwenden:

1. Öffnen Sie das Programmhauptfenster.
2. Wählen Sie auf der linken Fensterseite den Abschnitt **Virensuche** (**Vollständige Suche**, **Schnelle Suche**).
3. Klicken Sie für den ausgewählten Abschnitt auf den Link mit der festgelegten Sicherheitsstufe.
4. Klicken Sie im folgenden Fenster im Block **Sicherheitsstufe** auf die Schaltfläche **Einstellungen**.
5. Aktivieren Sie im folgenden Fenster auf der Registerkarte **Erweitert** im Block **Untersuchungstechnologien** die Verwendung der entsprechenden Technologie.

LEISTUNG DES COMPUTERS BEIM AUSFÜHREN VON AUFGABEN

Um die Belastung des Prozessors und der Laufwerkssubsysteme zu reduzieren, können Sie festlegen, dass Aufgaben zur Virensuche aufgeschoben werden.

Das Ausführen von Untersuchungsaufgaben erhöht die Auslastung des Prozessors und der Laufwerkssubsysteme und verlangsamt dadurch die Arbeit anderer Programme. In der Grundeinstellung hält Kaspersky Anti-Virus beim Eintreten dieser Situation die Ausführung von Untersuchungsaufgaben an und gibt Systemressourcen für Benutzeranwendungen frei.

Allerdings existiert eine Reihe von Programmen, die gestartet werden, wenn Prozessorressourcen frei werden, und die im Hintergrundmodus arbeiten. Wenn die Untersuchung von der Arbeit solcher Programme unabhängig sein soll, sollten ihnen keine Systemressourcen überlassen werden.

Beachten Sie, dass dieser Parameter für jede Untersuchungsaufgabe individuell angepasst werden kann. In diesem Fall besitzt der für eine konkrete Aufgabe festgelegte Parameter die höchste Priorität.

- *Gehen Sie folgendermaßen vor, damit Untersuchungsaufgaben zurückgestellt werden, wenn sie die Arbeit anderer Programme verlangsamen:*

1. Öffnen Sie das Programmhauptfenster.
2. Wählen Sie auf der linken Fensterseite den Abschnitt **Virensuche** (**Vollständige Suche**, **Schnelle Suche**).
3. Klicken Sie für den ausgewählten Abschnitt auf den Link mit der festgelegten Sicherheitsstufe.
4. Klicken Sie im folgenden Fenster im Block **Sicherheitsstufe** auf die Schaltfläche **Einstellungen**.
5. Aktivieren Sie im folgenden Fenster auf der Registerkarte **Erweitert** im Block **Untersuchungsmethoden** das Kontrollkästchen ☑ **Ressourcen für andere Anwendungen freigeben**.

AUFGABE ANHALTEN: ERSTELLEN EINES ZEITPLANS

Bei der Ausführung von Arbeiten, die die Betriebssystemressourcen stark beanspruchen, können Sie die Arbeit einer Untersuchungsaufgabe vorübergehend anhalten. Um die Belastung zu verringern und den schnellen Zugriff auf Objekte zu gewährleisten, können Sie in den Einstellungen festlegen, dass die Komponente für einen bestimmten Zeitraum angehalten wird.

- *Gehen Sie folgendermaßen vor, um den Zeitplan für das Anhalten einer Aufgabe anzupassen:*

1. Öffnen Sie das Programmhauptfenster.
2. Wählen Sie auf der linken Fensterseite den Abschnitt **Virensuche** (**Vollständige Suche**, **Schnelle Suche**).
3. Klicken Sie für den ausgewählten Abschnitt auf den Link mit der festgelegten Sicherheitsstufe.
4. Wählen Sie im Kontextmenü den Punkt **Einstellungen**.
5. Aktivieren Sie im folgenden Fenster auf der Registerkarte **Erweitert** im Block **Aufgabe anhalten** das Kontrollkästchen **Nach Zeitplan** und klicken Sie auf die Schaltfläche **Zeitplan**.
6. Legen Sie im Fenster **Aufgabe anhalten** (in den Feldern **Anhalten um** und **Fortsetzen um**) den Zeitraum fest, für den der Schutz angehalten werden soll (im Format HH:MM).

KOMPONENTE ANHALTEN: LISTE DER PROGRAMME ERSTELLEN

Bei der Ausführung von Arbeiten, die die Betriebssystemressourcen stark beanspruchen, können Sie die Arbeit einer Untersuchungsaufgabe vorübergehend anhalten. Um die Belastung zu verringern und den schnellen Zugriff auf Objekte zu gewährleisten, können Sie in den Einstellungen festlegen, dass die Komponente bei der Arbeit mit bestimmten Programmen angehalten wird.

Gehen Sie folgendermaßen vor, um festzulegen, dass die Aufgabe angehalten wird, während die angegebenen Programme arbeiten:

1. Öffnen Sie das Programmhauptfenster.
2. Wählen Sie auf der linken Fensterseite den Abschnitt **Virensuche** (**Vollständige Suche**, **Schnelle Suche**).
3. Klicken Sie für den ausgewählten Abschnitt auf den Link mit der festgelegten Sicherheitsstufe.
4. Wählen Sie im Kontextmenü den Punkt **Einstellungen**.
5. Aktivieren Sie im folgenden Fenster auf der Registerkarte .**Erweitert** im Block **Aufgabe anhalten** das Kontrollkästchen **Beim Start bestimmter Anwendungen** und klicken Sie auf die Schaltfläche W**ählen**.
6. Legen Sie im Fenster **Programme** die Liste der Programme an, bei deren Arbeit die Komponente angehalten werden soll.

STARTMODUS: FESTLEGEN EINES BENUTZERKONTOS

Sie können ein Benutzerkonto festlegen, mit dessen Rechten die Untersuchung ausgeführt werden soll.

Gehen Sie folgendermaßen vor, damit die Aufgabe mit den Rechten eines anderen Benutzerkontos gestartet wird:

1. Öffnen Sie das Programmhauptfenster.
2. Wählen Sie auf der linken Fensterseite den Abschnitt **Virensuche** (**Vollständige Suche**, **Schnelle Suche**).
3. Klicken Sie für den ausgewählten Abschnitt auf den Link mit der festgelegten Sicherheitsstufe.
4. Klicken Sie im folgenden Fenster im Block **Sicherheitsstufe** auf die Schaltfläche **Einstellungen**.
5. Aktivieren Sie im folgenden Fenster auf der Registerkarte **Startmodus** im Block **Benutzer** das Kontrollkästchen ☑ **Aufgabe starten mit Rechten des Benutzerkontos**. Geben Sie in den Feldern unten den Namen des Benutzerkontos und das Kennwort an.

STARTMODUS: ERSTELLEN EINES ZEITPLANS

Alle Aufgaben zur Virensuche können manuell oder nach einem festgelegten Zeitplan gestartet werden.

Standardmäßig ist für Aufgaben, die bei der Programminstallation erstellt wurden, der automatische Start nach Zeitplan deaktiviert. Eine Ausnahme bildet die Aufgabe zur schnellen Untersuchung, die jedes Mal beim Hochfahren des Computers ausgeführt wird.

Beim Erstellen eines Zeitplans für den Aufgabenstart muss die Frequenz, mit der die Untersuchung ausgeführt werden soll, festgelegt werden.

Wenn der Aufgabenstart aus einem bestimmten Grund nicht möglich war (wenn beispielsweise der Computer zum betreffenden Zeitpunkt ausgeschaltet war), können Sie festlegen, dass der Start automatisch erfolgt, sobald dies möglich ist.

Gehen Sie folgendermaßen vor, um den Startzeitplan einer Untersuchungsaufgabe anzupassen:

1. Öffnen Sie das Programmhauptfenster.
2. Wählen Sie auf der linken Fensterseite den Abschnitt **Virensuche** (**Vollständige Suche**, **Schnelle Suche**).
3. Klicken Sie für den ausgewählten Abschnitt auf den Link mit der festgelegten Sicherheitsstufe.
4. Klicken Sie im folgenden Fenster im Block **Startmodus** auf die Schaltfläche **Ändern**.
5. Nehmen Sie im folgenden Fenster **Zeitplan** die erforderlichen Änderungen vor.

Gehen Sie folgendermaßen vor, um den automatischen Start einer übersprungenen Aufgabe anzupassen:

1. Öffnen Sie das Programmhauptfenster.
2. Wählen Sie auf der linken Fensterseite den Abschnitt **Virensuche** (**Vollständige Suche**, **Schnelle Suche**).
3. Klicken Sie für den ausgewählten Abschnitt auf den Link mit der festgelegten Sicherheitsstufe.
4. Klicken Sie im folgenden Fenster im Block **Startmodus** auf die Schaltfläche **Ändern**.
5. Aktivieren Sie im folgenden Fenster **Zeitplan** im Block **Zeitplaneinstellungen** das Kontrollkästchen **Übersprungene Aufgabe starten**.

BESONDERHEITEN BEIM START EINER UNTERSUCHUNGSAUFGABE NACH ZEITPLAN

Alle Aufgaben zur Virensuche können manuell oder nach einem festgelegten Zeitplan gestartet werden.

Für Aufgaben, die nach einem festgelegten Zeitplan gestartet werden, können Sie eine zusätzliche Option verwenden: *Geplante Untersuchung anhalten, wenn Bildschirmschoner inaktiv oder Computer nicht blockiert ist*. Diese Option erlaubt es, den Start einer Aufgabe zurückzustellen, bis der Benutzer seine Arbeit auf dem Computer beendet hat. Dadurch wird verhindert, dass eine Untersuchungsaufgabe Computerressourcen verbraucht, während diese für andere Aufgaben benötigt werden.

Gehen Sie folgendermaßen vor, damit die Untersuchung erst gestartet wird, nachdem der Benutzer seine Arbeit beendet hat:

1. Öffnen Sie das Programmhauptfenster.
2. Wählen Sie auf der linken Fensterseite den Abschnitt **Vollständige Suche** oder **Schnelle Suche**.
3. Klicken Sie für den ausgewählten Abschnitt auf den Link mit der festgelegten Sicherheitsstufe.
4. Aktivieren Sie im folgenden Fenster im Block **Startmodus** das Kontrollkästchen **Geplante Untersuchung anhalten, wenn Bildschirmschoner inaktiv oder Computer nicht blockiert ist**.

STATISTIK ÜBER DIE VIRENSUCHE

Zusammenfassende Informationen über die Arbeit jeder Aufgabe zur Virensuche werden im Statistikfenster angezeigt. Hier können Sie erfahren, wie viele Objekte untersucht wurden, wie viele gefährliche Objekte und Objekte, deren Verarbeitung erforderlich ist, gefunden wurden. Außerdem werden hier Informationen über die Start- und Abschlusszeit der letzten Aufgabenausführung und über die Untersuchungsdauer angezeigt.

Die grundlegenden Informationen über die Untersuchungsergebnisse sind auf Registerkarten angeordnet:

- Die Registerkarte *Gefunden* nennt alle gefährlichen Objekte, die bei der Aufgabenausführung gefunden wurden.
- Die Registerkarte *Ereignisse* enthält eine vollständige Liste der Ereignisse, die bei der Aufgabenausführung aufgetreten sind.
- Die Registerkarte *Statistik* bietet statistische Daten zu den untersuchten Objekten.
- Die Registerkarte *Einstellungen* enthält die Parameter, mit denen die Aufgabe ausgeführt wird.

Wenn aufgrund der Ausführung einer Aufgabe ein Fehler auftritt, versuchen Sie die Aufgabe neu zu starten. Sollte der Versuch fehlerhaft abgeschlossen werden, dann speichern Sie den Bericht über die Aufgabenausführung mit Hilfe der Schaltfläche **Speichern unter** in einer Datei. Schicken Sie dann den Bericht an den Technischen Support-Service. Die Spezialisten von Kaspersky Lab werden Ihnen bei der Lösung des Problems helfen.

➧ *Gehen Sie folgendermaßen vor, um eine Statistik über die Ausführung einer Untersuchungsaufgabe anzuzeigen:*

1. Öffnen Sie das Programmhauptfenster.
2. Wählen Sie auf der linken Fensterseite den Abschnitt **Virensuche** (**Vollständige Suche**, **Schnelle Suche**), erstellen Sie eine Untersuchungsaufgabe und starten Sie diese zur Ausführung. Der Ausführungsfortschritt wird im Hauptfenster dargestellt. Klicken Sie auf den Link **Details**, um in das Statistikfenster zu gelangen.

FESTLEGEN EINHEITLICHER UNTERSUCHUNGSPARAMETER FÜR ALLE AUFGABEN

Jede Untersuchungsaufgabe wird mit ihren eigenen Parametern ausgeführt. Für die Aufgaben, die bei der Programminstallation auf dem Computer erstellt wurden, gelten standardmäßig die von den Kaspersky-Lab-Spezialisten empfohlenen Parameter.

Sie können einheitliche Untersuchungsparameter für alle Aufgaben festlegen. Als Grundlage gilt dabei die Auswahl der Parameter, die bei der Virenuntersuchung eines einzelnen Objekts verwendet werden.

➧ *Gehen Sie folgendermaßen vor, um einheitliche Untersuchungsparameter für alle Aufgaben festzulegen:*

1. Öffnen Sie das Programmkonfigurationsfenster.
2. Wählen Sie auf der linken Fensterseite den Abschnitt **Virensuche**.
3. Klicken Sie auf der rechten Fensterseite im Block **Einstellungen anderer Aufgaben** auf die Schaltfläche **Übernehmen**. Bestätigen Sie im Bestätigungsfenster das Übernehmen der einheitlichen Parameter.

STANDARDMÄßIGE UNTERSUCHUNGSEINSTELLUNGEN WIEDERHERSTELLEN

Während der Konfiguration der Parameter für die Aufgabenausführung können Sie jederzeit zu den empfohlenen Einstellungen zurückkehren. Diese gelten als optimal, werden von den Kaspersky-Lab-Spezialisten empfohlen und sind in der Sicherheitsstufe **Empfohlen** zusammengefasst.

➧ *Gehen Sie folgendermaßen vor, um die standardmäßigen Untersuchungseinstellungen für Objekte wiederherzustellen,*

1. Öffnen Sie das Programmhauptfenster.
2. Wählen Sie auf der linken Fensterseite den Abschnitt **Virensuche** (**Vollständige Suche**, **Schnelle Suche**).

3. Klicken Sie für den ausgewählten Abschnitt auf den Link mit der festgelegten Sicherheitsstufe.
4. Klicken Sie im folgenden Fenster im Block **Sicherheitsstufe** auf die Schaltfläche **Grundeinstellung**.

PROGRAMM-UPDATE

Eine Voraussetzung für die Sicherheit ist die Pflege des aktuellen Zustands von Kaspersky Anti-Virus. Jeden Tag tauchen neue Viren, trojanische und andere schädliche Programme auf. Deshalb ist es sehr wichtig sicherzustellen, dass Ihre Informationen zuverlässig geschützt werden.

Die Aktualisierung des Programms umfasst den Download und die Installation folgender Elemente auf den Server:

- **Programm-Datenbanken**

  Der Schutz der Informationen auf ihrem Computer basiert auf Programm-Datenbanken. Datei-Anti-Virus verwendet diese bei der Suche und Desinfektion gefährlicher Objekte auf dem Server. Die Datenbanken werden stündlich durch Einträge über neue Bedrohungen und entsprechende Desinfektionsmethoden ergänzt. Deshalb wird ausdrücklich empfohlen, die Datenbanken regelmäßig zu aktualisieren.

- **Programm-Module**

  Neben den Programm-Datenbanken können auch die Programm-Module aktualisiert werden. Updatepakete beheben Schwachstellen von Kaspersky Anti-Virus, fügen neue Funktionen hinzu und optimieren bestehende Funktionen.

Als standardmäßige Updatequelle für Kaspersky Anti-Virus gelten die speziellen Kaspersky-Lab-Updateserver.

Um die Updates von den Servern herunterzuladen, ist eine Verbindung Ihres Computers mit dem Internet erforderlich. In der Grundeinstellung wird die Internetverbindung automatisch ermittelt. Wenn die Proxyserver-Einstellungen nicht automatisch ermittelt werden, passen Sie die Parameter der Verbindung mit dem Proxyserver an.

Bei der Aktualisierung werden die Programm-Module und Datenbanken auf dem Server mit den auf der Updatequelle vorhandenen verglichen. Wenn auf dem Server die aktuelle Version der Datenbanken und Module installiert ist, erscheint auf dem Bildschirm eine Meldung darüber, dass der Schutz auf dem Computer aktuell ist. Wenn Datenbanken und Module nicht aktuell sind, wird nur der fehlende Teil der Updates auf dem Server installiert. Datenbanken und Module werden nicht vollständig kopiert, wodurch die Updategeschwindigkeit wesentlich gesteigert und der Netzwerkverkehr entlastet wird.

Bevor die Datenbanken aktualisiert werden, legt Kaspersky Anti-Virus eine Sicherungskopie davon an. Bei Bedarf können Sie zu den vorhergehenden Datenbanken zurückkehren.

Die Option zum Rollback des Updates ist beispielsweise erforderlich, wenn Sie die Datenbanken aktualisiert haben und diese bei der Arbeit beschädigt wurden. Sie können zu der vorherigen Variante der Datenbanken zurückkehren und die Aktualisierung später erneut versuchen.

Während die Anwendung aktualisiert wird, können die heruntergeladenen Updates gleichzeitig in eine lokale Quelle kopiert werden. Dieser Dienst erlaubt es, die Datenbanken und Module des Programms auf Netzwerkcomputern zu aktualisieren und dabei Netzwerkverkehr einzusparen.

Zusätzlich kann der Modus für den automatischen Start des Updates angepasst werden.

Im Abschnitt **Update** werden Informationen über den aktuellen Zustand der Programm-Datenbanken angezeigt.

Sie können zum Bericht über das Update wechseln, der vollständige Informationen über die Ereignisse, die bei der Ausführung von Updateaufgaben eingetreten sind, bietet. Außerdem können Sie auf der Seite www.kaspersky.de einen Überblick über die Virenaktivität erhalten (Link **Überblick über die Virenaktivität**).

➡ *Gehen Sie folgendermaßen vor, um die Parameter einer bestimmten Updateaufgabe zu ändern:*

1. Öffnen Sie das Programmhauptfenster.

2. Wählen Sie auf der linken Fensterseite den Abschnitt **Update**.

3. Klicken Sie für den ausgewählten Abschnitt auf den Link mit dem festgelegten Startmodus.

4. Nehmen Sie im folgenden Fenster in den Einstellungen der gewählten Aufgabe die erforderlichen Änderungen vor.

Gehen Sie folgendermaßen vor, um zum Updatebericht zu gelangen:

1. Öffnen Sie das Programmhauptfenster.

2. Wählen Sie auf der linken Fensterseite den Abschnitt **Update**.

3. Klicken Sie auf die Schaltfläche **Berichte**.

IN DIESEM ABSCHNITT

START DES UPDATES

Sie können das Programm-Update jederzeit starten. Die Aktualisierung erfolgt aus der von Ihnen gewählten Updatequelle.

Das Update von Kaspersky Anti-Virus kann auf zwei Arten gestartet werden:

- aus dem Kontextmenü.
- aus dem Programmhauptfenster.

Der Updateprozess der Anwendung wird im Programmhauptfenster dargestellt.

Beachten Sie, dass beim Ausführen des Updates gleichzeitig die Update-Verteilung aus einer lokalen Quelle erfolgt, falls dieser Dienst aktiviert wurde.

- *Gehen Sie folgendermaßen vor, um das Update von Kaspersky Anti-Virus aus dem Kontextmenü zu starten:*

  1. Klicken Sie im Infobereich der Taskleiste mit der rechten Maustaste auf das Programmsymbol.
  2. Wählen Sie im Kontextmenü den Punkt **Update** aus.

- *Gehen Sie folgendermaßen vor, um das Update aus dem Hauptfenster von Kaspersky Anti-Virus zu starten,*

  1. Öffnen Sie das Programmhauptfenster.
  2. Wählen Sie auf der linken Fensterseite den Abschnitt **Update**.
  3. Klicken Sie auf die Schaltfläche **Update ausführen**. Der Ausführungsfortschritt der Aufgabe wird im Programmhauptfenster dargestellt.

ROLLBACK ZUM VORHERIGEN UPDATE

Jedes Mal, wenn Sie das Update starten, erstellt Kaspersky Anti-Virus zuerst eine Sicherungskopie der bisher verwendeten Datenbanken und Programm-Module und beginnt danach mit der Aktualisierung. Dadurch wird Ihnen erlaubt, zur Verwendung der vorherigen Datenbanken zurückzukehren, wenn das Update erfolglos sein sollte.

Die Rollback-Funktion ist beispielsweise nützlich, wenn die Datenbanken teilweise beschädigt wurden. Lokale Datenbanken können entweder von einem Benutzer oder von einem bösartigen Programm beschädigt werden. Eine Beschädigung ist nur möglich, wenn der Selbstschutz des Programms deaktiviert wurde. Sie können zu den vorherigen Datenbanken zurückkehren und die Aktualisierung später erneut versuchen.

- *Gehen Sie folgendermaßen vor, um zur Verwendung der vorhergehenden Version der Datenbanken zurückzukehren:*

  1. Öffnen Sie das Programmhauptfenster.
  2. Wählen Sie auf der linken Fensterseite den Abschnitt **Update**.
  3. Klicken Sie auf den Link **Rollback zu den vorherigen Datenbanken**.

AUSWAHL DER UPDATEQUELLE

Eine *Updatequelle* ist eine Ressource, die Updates für die Datenbanken und Module von Kaspersky Anti-Virus enthält.

Als Updatequelle können Sie verwenden:

- *Administrationsserver* – zentralisierter Updatespeicher, der sich auf dem Administrationsserver von Kaspersky Administration Kit befindet (Details siehe Administratorhandbuch zu "Kaspersky Administration Kit").
- *Updateserver von Kaspersky Lab* – spezielle Internetseiten, auf denen Updates der Datenbanken und Anwendungsmodule für alle Kaspersky-Lab-Produkte zur Verfügung stehen.
- *HTTP- oder FTP-Server, lokale Ordner oder Netzwerkordner* – lokaler Server oder Ordner, der die aktuellen Updates enthält.

Wenn Sie keinen Zugriff auf die Kaspersky-Lab-Updateserver besitzen (wenn beispielsweise kein Internetzugang vorhanden ist), können Sie unter den Nummern +7 (495) 797-87-00 und +7 (495) 645-79-39 unsere Hauptverwaltung anrufen. Dort können Sie die Adressen der Partner von Kaspersky Lab erfahren, die Ihnen die Updates auf Disketten oder CDs im zip-Format anbieten können.

Updates, die sich auf einem Wechseldatenträger befinden, können Sie auf einer ftp- oder http-Seite oder in einem lokalen oder Netzwerkordner speichern.

Geben Sie zur Bestellung von Updates auf Wechseldatenträgern unbedingt an, ob Sie Updates für die Programm-Module erhalten möchten.

Wenn Sie als Updatequelle eine Ressource gewählt haben, die sich außerhalb des lokalen Netzwerks befindet, ist für die Aktualisierung eine Internetverbindung erforderlich.

Wenn mehrere Ressourcen als Updatequellen gewählt wurden, greift das Programm bei der Aktualisierung streng nach der Listenreihenfolge darauf zu und aktualisiert sich von der ersten verfügbaren Quelle.

Gehen Sie folgendermaßen vor, um eine Updatequelle auszuwählen:

1. Öffnen Sie das Programmhauptfenster.
2. Wählen Sie auf der linken Fensterseite den Abschnitt **Update**.
3. Klicken Sie für den ausgewählten Abschnitt auf den Link mit dem festgelegten Startmodus.
4. Klicken Sie im folgenden Fenster im Block **Updateparameter** auf die Schaltfläche **Einstellungen**.
5. Klicken Sie im folgenden Fenster auf der Registerkarte **Updatequelle** auf die Schaltfläche **Hinzufügen**.
6. Wählen Sie im folgenden Fenster **Updatequelle wählen** eine ftp- oder http-Seite oder geben Sie ihre IP-Adresse, den symbolischen Namen oder die URL-Adresse an.

REGIONSEINSTELLUNGEN

Wenn Sie die Kaspersky-Lab-Server als Updatequelle verwenden, kann der für Sie günstigste Standort des Servers für den Update-Download ausgewählt werden. Kaspersky Lab verfügt in mehreren Ländern der Erde über Server. Die Auswahl des geografisch am nächsten gelegenen Kaspersky-Lab-Updateservers kann die Dauer des Updates verkürzen und die Downloadgeschwindigkeit erhöhen.

Gehen Sie folgendermaßen vor, um am nächsten gelegenen Server auszuwählen:

1. Öffnen Sie das Programmhauptfenster.
2. Wählen Sie auf der linken Fensterseite den Abschnitt **Update**.
3. Klicken Sie für den ausgewählten Abschnitt auf den Link mit dem festgelegten Startmodus.
4. Klicken Sie im folgenden Fenster im Block **Updateparameter** auf die Schaltfläche **Einstellungen**.
5. Wählen Sie im folgenden Fenster auf der Registerkarte **Updatequelle** im Block **Regionsoptionen** die Variante **Aus der Liste wählen** und wählen Sie aus der Dropdown-Liste das Land aus, in dem Sie sich gerade aufhalten.

   Wenn die Variante **Automatisch ermitteln** gewählt wurde, werden beim Update Informationen über den aktuellen Standort aus der Registrierung des Betriebssystems verwendet.

VERWENDUNG EINES PROXYSERVERS

Wenn die Internetverbindung über einen Proxyserver erfolgt, ist es erforderlich, seine Parameter anzupassen.

Gehen Sie folgendermaßen vor, um die Proxyserver-Parameter anzupassen:

1. Öffnen Sie das Programmhauptfenster.

2. Wählen Sie auf der linken Fensterseite den Abschnitt **Update**.

3. Klicken Sie für den ausgewählten Abschnitt auf den Link mit dem festgelegten Startmodus.

4. Klicken Sie im folgenden Fenster im Block **Updateparameter** auf die Schaltfläche **Einstellungen**.

5. Passen Sie im folgenden Fenster auf der Registerkarte **Proxy-Einstellungen** die Parameter für den Proxyserver an.

STARTMODUS: FESTLEGEN EINES BENUTZERKONTOS

In Kaspersky Anti-Virus ist ein Dienst zum Start des Programm-Updates unter einem anderen Benutzerkonto (Impersonalisierung) realisiert. Dieser Dienst ist standardmäßig deaktiviert und Aufgaben werden unter dem aktiven Benutzerkonto gestartet, mit dem Sie sich am System angemeldet haben.

Da das Programm-Update aus einer Quelle erfolgen kann, auf die Sie möglicherweise keinen Zugriff (beispielsweise ein Netzwerkverzeichnis für Updates) oder keine Rechte eines autorisierten Benutzers für einen Proxyserver besitzen, können Sie diesen Dienst benutzen, um das Programm-Update unter dem Namen eines Benutzers zu starten, der über die erforderlichen Privilegien verfügt.

Beachten Sie, dass die zeitplangesteuerte Aktualisierung mit den Rechten des aktiven Benutzerkontos ausgeführt wird, wenn der Start mit Rechten eines anderen Benutzers nicht aktiviert wurde. Sollte es vorkommen, dass zu einem bestimmten Zeitpunkt kein Benutzer auf dem Computer angemeldet ist und der Updatestart nicht mit Rechten eines anderen Benutzers geplant wurde, dann wird das Update dem Zeitplan entsprechend mit den Rechten des Benutzers SYSTEM gestartet.

- *Gehen Sie folgendermaßen vor, damit die Aufgabe mit den Rechten eines anderen Benutzerkontos gestartet wird:*

1. Öffnen Sie das Programmhauptfenster.

2. Wählen Sie auf der linken Fensterseite den Abschnitt **Update**.

3. Klicken Sie für den ausgewählten Abschnitt auf den Link mit dem festgelegten Startmodus.

4. Klicken Sie im folgenden Fenster im Block **Updateparameter** auf die Schaltfläche **Einstellungen**.

5. Aktivieren Sie im folgenden Fenster auf der Registerkarte **Erweitert** im Block **Startmodus** das Kontrollkästchen ☑ **Aufgabe starten mit Rechten des Benutzerkontos**. Geben Sie darunter die Daten des Benutzerkontos an, unter dem die Aufgabe gestartet werden soll: Name des Benutzerkontos und Kennwort.

STARTMODUS: ERSTELLEN EINES ZEITPLANS

Alle Aufgaben zur Virensuche können manuell oder nach einem festgelegten Zeitplan gestartet werden.

Beim Erstellen eines Zeitplans für den Aufgabenstart muss die Frequenz, mit der das Update ausgeführt werden soll, festgelegt werden.

Wenn der Aufgabenstart aus einem bestimmten Grund nicht möglich war (wenn beispielsweise der Computer zum betreffenden Zeitpunkt ausgeschaltet war), können Sie festlegen, dass der Start ausgeführt wird, sobald dies möglich ist.

- *Gehen Sie folgendermaßen vor, um den Startzeitplan einer Untersuchungsaufgabe anzupassen:*

1. Öffnen Sie das Programmhauptfenster.

2. Wählen Sie auf der linken Fensterseite den Abschnitt **Update**.

3. Klicken Sie für den ausgewählten Abschnitt auf den Link mit dem festgelegten Startmodus.

4. Klicken Sie im folgenden Fenster im Block **Startmodus** auf die Schaltfläche **Ändern**.

5. Nehmen Sie im folgenden Fenster **Zeitplan** die erforderlichen Änderungen vor.

Gehen Sie folgendermaßen vor, um den automatischen Start einer übersprungenen Aufgabe anzupassen:

1. Öffnen Sie das Programmhauptfenster.

2. Wählen Sie auf der linken Fensterseite den Abschnitt **Update**.

3. Klicken Sie für den ausgewählten Abschnitt auf den Link mit dem festgelegten Startmodus.

4. Klicken Sie im folgenden Fenster im Block **Startmodus** auf die Schaltfläche **Ändern**.

5. Aktivieren Sie im folgenden Fenster **Zeitplan** im Block **Zeitplaneinstellungen** das Kontrollkästchen **Übersprungene Aufgabe starten**.

AUSWAHL DES UPDATEOBJEKTS

Das Update-Objekt bestimmt, was genau aktualisiert wird:

- Programm-Datenbanken.
- Programm-Module.

Die Programm-Datenbanken werden immer aktualisiert, die Programm-Module nur dann, wenn der entsprechende Modus aktiviert ist.

Wenn im Augenblick der Aktualisierung ein Paket für die Programm-Module in der Quelle vorhanden ist, lädt Kaspersky Anti-Virus es herunter und installiert es nach dem Neustart des Computers. Die heruntergeladenen Updates für Module werden nicht erst nach dem Neustart installiert.

Sollte die nächste Aktualisierung stattfinden, bevor der Computer neu gestartet und die zuvor heruntergeladenen Updates der Programm-Module installiert wurden, dann werden nur die Bedrohungssignaturen aktualisiert.

Gehen Sie folgendermaßen vor, damit beim Updateprozess die Updates der Programm-Module auf Ihren Computer kopiert und installiert werden:

1. Öffnen Sie das Programmhauptfenster.

2. Wählen Sie auf der linken Fensterseite den Abschnitt **Update**.

3. Klicken Sie für den ausgewählten Abschnitt auf den Link mit dem festgelegten Startmodus.

4. Aktivieren Sie im folgenden Fenster im Block **Updateparameter** das Kontrollkästchen **Programm-Module aktualisieren**.

ÄNDERN DES STARTMODUS FÜR DIE UPDATEAUFGABE

Der Startmodus für das Update von Kaspersky Anti-Virus wird im Konfigurationsassistenten des Programms (s. Abschnitt "Anpassen der Parameter für das Update" auf S. 27) festgelegt. Sie können den festgelegten Startmodus ändern.

Für den Start der Updateaufgabe stehen folgende Modi zur Auswahl:

- **Automatisch**. Kaspersky Anti-Virus prüft in festgelegten Zeitabständen, ob an der Updatequelle ein neues Updatepaket vorhanden ist. Wenn neue Updates vorhanden sind, lädt Kaspersky Anti-Virus sie herunter und installiert sie auf dem Computer. Dieser Updatemodus wird standardmäßig benutzt.

Kaspersky Anti-Virus führt in dem Intervall, das im vorhergehenden Updatepaket angegeben ist, einen Updateversuch durch. Dadurch wird erlaubt, die Updatefrequenz bei Viren-Epidemien und in anderen gefährlichen Situationen automatisch zu regulieren. Das Programm wird rechtzeitig mit aktuellen Updates für die Datenbanken, für Angriffssignaturen und für die Programm-Module versorgt, wodurch das Eindringen gefährlicher Programme auf Ihren Computer verhindert wird.

- **Nach Zeitplan** (Das Intervall ist von den Zeitplaneinstellungen abhängig). Das Update wird automatisch nach einem festgelegten Zeitplan gestartet.

- **Manuell**. In diesem Fall starten Sie die Aktualisierung des Programms selbständig. Kaspersky Anti-Virus informiert Sie bei Bedarf über die Notwendigkeit der Aktualisierung.

Gehen Sie folgendermaßen vor, um den Startmodus für die Updateaufgabe anzupassen:

1. Öffnen Sie das Programmhauptfenster.
2. Wählen Sie auf der linken Fensterseite den Abschnitt **Update**.
3. Klicken Sie für den ausgewählten Abschnitt auf den Link mit dem festgelegten Startmodus.
4. Wählen Sie im folgenden Fenster im Block **Startmodus** einen Startmodus für die Updateaufgabe. Wenn Sie den Modus der zeitplangesteuerteт Aktualisierung wählen, erstellen sie einen Zeitplan.

UPDATE AUS EINEM LOKALEN ORDNER

Die Update-Verteilung aus einem lokalen Ordner wird folgendermaßen organisiert:

1. Ein Computer des Netzwerks lädt das Paket mit den Updates für Kaspersky Anti-Virus von den Kaspersky-Lab-Webservern im Internet oder einer anderen Webressource, auf der sich die aktuellen Updates befinden, herunter. Die heruntergeladenen Updates werden in einem gemeinsamen Ordner abgelegt.
2. Die übrigen Netzwerkcomputer verwenden den gemeinsamen Ordner, um die Updates für das Programm herunterzuladen.

Kaspersky Anti-Virus 6.0 erhält von den Kaspersky-Lab-Updateservern nur das ihm entsprechende Updatepaket. Es wird empfohlen, die Update-Verteilung für andere Kaspersky-Lab-Anwendungen über Kaspersky Administration Kit vorzunehmen.

Gehen Sie folgendermaßen vor, um den Modus für die Update-Verteilung zu aktivieren:

1. Öffnen Sie das Programmhauptfenster.
2. Wählen Sie auf der linken Fensterseite den Abschnitt **Update**.
3. Klicken Sie für den ausgewählten Abschnitt auf den Link mit dem festgelegten Startmodus.
4. Klicken Sie im folgenden Fenster auf die Schaltfläche **Einstellungen**.
5. Aktivieren Sie im folgenden Fenster auf der Registerkarte **Erweitert** im Block **Update-Verteilung** das Kontrollkästchen **Updates in folgenden Ordner kopieren** und geben Sie im Feld darunter den gemeinsamen Ordner an, in dem heruntergeladene Updates gespeichert werden sollen. Weiterhin kann man den Pfad im Fenster auswählen, das sich mit der Schaltfläche **Durchsuchen** öffnen lässt.

Damit das Update aus dem gewählten gemeinsamen Ordner erfolgt, nehmen Sie auf allen Computern des Netzwerks folgende Einstellungen vor:

1. Öffnen Sie das Programmhauptfenster.
2. Wählen Sie auf der linken Fensterseite den Abschnitt **Update**.

3. Klicken Sie für den ausgewählten Abschnitt auf den Link mit dem festgelegten Startmodus.

4. Klicken Sie im folgenden Fenster auf die Schaltfläche **Einstellungen**.

5. Klicken Sie im folgenden Fenster auf der Registerkarte **Updatequelle** auf die Schaltfläche **Hinzufügen**.

6. Wählen Sie im folgenden Fenster **Updatequelle** wählen den Ordner aus oder geben im Feld **Quelle** den vollständigen Pfad an.

7. Deaktivieren Sie auf der Registerkarte **Updatequelle** das Kontrollkästchen ☑ **Kaspersky-Lab-Updateserver**.

STATISTIK FÜR DAS UPDATE

Zusammenfassende Informationen über die Arbeit der Updateaufgaben werden im Statistikfenster angezeigt. Hier können Sie feststellen, welche Ereignisse bei der Aufgabenausführung aufgetreten sind (Registerkarte *Ereignisse*), und Sie können eine Liste der Einstellungen ansehen, mit denen eine Aufgabe ausgeführt wird (Registerkarte *Einstellungen*).

Wenn aufgrund der Ausführung einer Aufgabe ein Fehler auftritt, versuchen Sie die Aufgabe neu zu starten. Sollte der Versuch fehlerhaft abgeschlossen werden, dann speichern Sie den Bericht über die Aufgabenausführung mit Hilfe der Schaltfläche **Speichern unter** in einer Datei. Schicken Sie dann den Bericht an den Technischen Support-Service. Die Spezialisten von Kaspersky Lab werden Ihnen bei der Lösung des Problems helfen.

Eine kurze Updatestatistik befindet sich im oberen Bereich des Statistikfensters. Sie enthält die Größe der kopierten und installierten Updates, die Geschwindigkeit, mit der das Update erfolgte, die Vorgangsdauer und andere Informationen.

➧ *Gehen Sie folgendermaßen vor, um eine Statistik über die Ausführung einer Untersuchungsaufgabe anzuzeigen:*

1. Öffnen Sie das Programmhauptfenster.

2. Wählen Sie auf der linken Fensterseite den Abschnitt **Update**, erstellen Sie eine Updateaufgabe und starten Sie diese zur Ausführung. Der Ausführungsfortschritt der Aufgabe wird im Hauptfenster dargestellt. Über den Link **Details** gelangen Sie zum Statistikfenster wechseln можно перейти в окно статистики.

MÖGLICHE PROBLEME BEIM UPDATE

Im Verlauf der Aktualisierung der Programm-Module von Kaspersky Anti-Virus oder der Bedrohungssignaturen können Fehler auftreten, die mit inkorrekten Update-Einstellungen, Verbindungsproblemen usw. zusammenhängen. Dieser Hilfeabschnitt beschreibt die meisten dieser Fehler und bietet Tipps zum Beheben der Fehler. Sollten Fehler auftreten, die nicht in der Hilfe beschrieben sind, oder sollten Sie weitergehende Hilfe zur Lösung von Problemen benötigen, dann versuchen Sie die Informationen in der Wissensdatenbank auf der Internetseite des Technischen Supports im Abschnitt "Das Programm hat einen Fehler gemeldet..." zu finden. Wenn die Empfehlungen, die in diesem Abschnitt dargestellt sind, das Problem zu lösen nicht geholfen haben oder diese Information in der Wissensdatenbank fehlt, dann wenden Sie sich bitte über das Webformular an den Technischen Support-Service.

KONFIGURATIONSFEHLER

Fehler dieser Gruppe treten hauptsächlich aufgrund der inkorrekten Installation der Anwendung oder nach einer Veränderung der Anwendungskonfiguration auf, durch die es zur Funktionsunfähigkeit der Anwendung kommen kann.

Generelle Empfehlungen:

Wenn ein Fehler dieser Gruppe auftritt, empfiehlt es sich, das Update erneut zu starten. Sollte sich der Fehler wiederholen, wenden Sie sich an den technischen Kundendienst.

Wenn das Problem mit der inkorrekten Installation der Anwendung zusammenhängt, wird empfohlen, die Anwendung neu zu installieren.

Es wurde keine Updatequelle festgelegt

Keine der Quellen enthält Dateien für das Update. Möglicherweise wurde in den Updateparametern keine Updatequelle angegeben. Prüfen Sie, ob die Updateparameter korrekt eingestellt sind, und wiederholen Sie den Versuch.

Fehler bei Lizenzüberprüfung

Dieser Fehler tritt auf, wenn die von der Anwendung verwendete Schlüsseldatei gesperrt ist oder auf der schwarzen Liste für Lizenzen steht.

Fehler beim Empfang von Updateparametern

Interner Fehler beim Download von Parametern der Updateaufgabe. Bitte prüfen Sie, ob die Updateparameter korrekt eingestellt sind, und wiederholen Sie den Versuch.

Unzureichende Rechte für das Update

Dieser Fehler tritt gewöhnlich auf, wenn das Benutzerkonto, in dessen Namen das Update gestartet wird, keine Zugriffsrechte für die Updatequelle oder den Ordner, in dem die Updates gespeichert sind, besitzt. Es wird empfohlen, das Vorhandensein der Rechte für dieses Benutzerkonto zu prüfen.

Dieser Fehler tritt auch auf, wenn versucht wird, Updatedateien in einen Ordner zu kopieren, der nicht erstellt werden kann.

Interner Fehler

Interner Logikfehler bei der Arbeit der Updateaufgabe. Bitte prüfen Sie, ob die Updateparameter korrekt eingestellt sind, und wiederholen Sie den Versuch.

Fehler bei Überprüfung des Updates

Dieser Fehler tritt auf, wenn Dateien, die von der Updatequelle heruntergeladen wurden, die interne Prüfung nicht bestehen. Bitte wiederholen Sie den Updateversuch später.

FEHLER, DIE BEI DER ARBEIT MIT ORDNERN UND DATEIEN AUFTRETEN KÖNNEN

Fehler dieser Gruppe treten auf, wenn das Benutzerkonto, in dessen Namen das Update gestartet wird, keine Zugriffsrechte für die Updatequelle oder den Ordner, in dem die Updates gespeichert sind, besitzt.

Generelle Empfehlungen:

Wenn Fehler dieser Gruppe auftreten, empfiehlt es sich, für dieses Benutzerkonto das Vorhandensein der Rechte für den Zugriff auf die betreffenden Dateien und Ordner zu prüfen.

Der Ordner kann nicht erstellt werden

Dieser Fehler tritt auf, wenn während des Ausführens des Updates ein Ordner nicht erstellt werden kann.

Unzureichende Rechte zum Ausführen einer Datei-Operation

Dieser Fehler tritt auf, wenn das Benutzerkonto, in dessen Namen das Update gestartet wird, nicht über die erforderlichen Rechte zum Ausführen von Operationen mit Dateien verfügt.

Datei oder Ordner nicht gefunden

Dieser Fehler tritt auf, wenn eine Datei oder ein Ordner fehlt, die/der beim Update benötigt wird. Es wird empfohlen, zu prüfen, ob die betreffende Datei bzw. der Ordner vorhanden und verfügbar ist.

Fehler bei Datei-Operation

Dieser Fehler ist ein interner Logikfehler des Updatemoduls beim Ausführen von Operationen mit Dateien.

NETZWERKFEHLER

Fehler dieser Gruppe treten auf, wenn Verbindungsprobleme oder fehlerhafte Einstellungen für die Netzwerkverbindung vorhanden sind.

Generelle Empfehlungen:

Wenn Fehler dieser Gruppe auftreten, empfiehlt es sich, die Verbindung Ihres Computers mit dem Netzwerk, die Korrektheit der Verbindungsparameter und die Verfügbarkeit der Updatequelle zu prüfen. Nehmen Sie danach einen erneuten Updateversuch vor. Sollte der Versuch erfolglos sein, wenden Sie sich an den technischen Kundendienst.

Netzwerkfehler

Im Verlauf des Downloads von Updatedateien ist ein Fehler aufgetreten. Wenn dieser Fehler auftritt, prüfen Sie die Verbindung Ihres Computers zum Netzwerk.

Die Verbindung wurde getrennt

Dieser Fehler tritt auf, wenn die Verbindung mit der Updatequelle aus bestimmten Gründen getrennt wurde.

Das Zeitlimit für Netzwerkoperationen ist abgelaufen

Die Wartezeit für die Verbindung mit der Updatequelle wurde überschritten. Beim Anpassen der Updateparameter für die Anwendung können Sie ein exaktes Zeitlimit für die Verbindung mit der Updatequelle festlegen. Wenn Ihr Computer innerhalb des festgelegten Zeitraums keine Verbindung mit dem Updateserver oder Updateordner herstellen kann, tritt dieser Fehler auf. Es wird empfohlen, in diesem Fall zu prüfen, ob der Updatedienst korrekt eingestellt und ob die Updatequelle verfügbar ist.

Autorisierungsfehler auf FTP-Server

Dieser Fehler tritt auf, wenn die Autorisierungsparameter für den FTP-Server, der als Updatequelle dient, fehlerhaft angegeben wurden. Bitte prüfen Sie, ob in den Parametern des FTP-Servers der Download von Dateien für dieses Benutzerkonto erlaubt ist.

Autorisierungsfehler auf Proxyserver

Dieser Fehler tritt auf, wenn in den Parametern für das Update über einen Proxyserver ein Benutzername und Kennwort oder ein Benutzerkonto, in dessen Namen das Update gestartet wird, angegeben wurde, das nicht über Zugriffsrechte für die Updatequelle verfügt. Bitte ändern Sie die Autorisierungsparameter und wiederholen Sie den Updateversuch.

Fehler bei Auflösung von DNS-Namen

Dieser Fehler tritt auf, wenn keine Updatequelle gefunden wurde. Möglicherweise wurde die Adresse der Updatequelle inkorrekt angegeben, die Parameter der Netzwerkverbindung sind fehlerhaft oder der DNS-Server ist nicht verfügbar. Es wird empfohlen, die Updateparameter und die Verfügbarkeit der Updatequelle zu prüfen und den Versuch danach zu wiederholen.

Verbindung mit Updatequelle kann nicht hergestellt werden

Dieser Fehler tritt auf, wenn keine Verbindung zur Updatequelle besteht. Bitte prüfen Sie, ob die Adresse der Updatequelle korrekt ist, und wiederholen Sie den Versuch.

Verbindung mit Proxyserver kann nicht hergestellt werden

Dieser Fehler tritt auf, wenn die Parameter für die Verbindung mit dem Proxyserver inkorrekt angegeben wurden. Um das Problem zu lösen, wird empfohlen, zu prüfen, ob diese Parameter korrekt sind, ob der Proxyserver und das Netzwerk verfügbar sind, und den Updateversuch zu wiederholen.

Fehler beim Auflösen des DNS-Namens für den Proxyserver

Dieser Fehler tritt auf, wenn kein Proxyserver gefunden wurde. Es wird empfohlen, zu prüfen, ob die Parameter für die Verbindung mit dem Proxyserver korrekt sind und ob Zugriff auf den DNS-Server besteht.

FEHLER, DIE MIT EINER BESCHÄDIGUNG DER DATENBANKEN VERBUNDEN SIND

Fehler dieser Gruppe gehen darauf zurück, dass die Updatequelle beschädigte Dateien enthält.

Generelle Empfehlungen:

Wenn das Update von den Kaspersky-Lab-Webservern erfolgt, versuchen Sie, das Update erneut zu starten. Sollte der Versuch erfolglos sein, wenden Sie sich an den technischen Kundendienst.

Beim Update aus einer anderen Quelle (beispielsweise aus einem lokalen Ordner) ist es empfehlenswert, den Inhalt der Updatequelle über die Kaspersky-Lab-Updateserver zu aktualisieren. Sollte der Fehler wiederholt auftreten, wenden Sie sich an den technischen Kundendienst.

Die Datei fehlt in der Updatequelle

Alle Dateien, die während des Updates auf Ihren Computer heruntergeladen und darauf installiert werden, sind in einer speziellen Datei aufgezählt, die im Paket enthalten ist. Dieser Fehler tritt auf, wenn eine bestimmte Datei auf der Liste der zu aktualisierenden Dateien steht, jedoch an der Updatequelle nicht vorhanden ist.

Fehler bei Signaturüberprüfung

Dieser Fehler kann von der Anwendung zurückgegeben werden, wenn die elektronische digitale Signatur des heruntergeladenen Updatepakets beschädigt ist oder nicht der Kaspersky-Lab-Signatur entspricht.

Die Indexdatei ist beschädigt oder fehlt

Dieser Fehler tritt auf, wenn die Indexdatei im Format xml, die für die Ausführung des Updates maßgeblich ist, an der Updatequelle nicht vorhanden ist.

FEHLER, DIE MIT DEM UPDATE VOM ADMINISTRATIONSSERVER FÜR KASPERSKY ADMINISTRATION KIT VERBUNDEN SIND

Fehler dieser Gruppe stehen damit in Verbindung, dass beim Update der Anwendung über den Administrationsserver für Kaspersky Administration Kit Probleme bestehen.

Generelle Empfehlungen:

Vergewissern Sie sich in erster Linie, dass die Anwendung Kaspersky Administration Kit und ihre Komponenten (Administrationsserver und Administrationsagent) installiert sind und gestartet wurden. Wiederholen Sie den Updateversuch. Wenn das Update fehlschlägt, starten Sie Administrationsagent und Administrationsserver neu und wiederholen Sie den Updateversuch noch einmal. Sollte sich das Problem nicht lösen lassen, wenden Sie sich an den Technischen Support-Service.

Fehler bei Verbindung mit Administrationsserver

Dieser Fehler tritt auf, wenn keine Verbindung mit dem Administrationsserver von Kaspersky Administration Kit möglich ist. Es wird empfohlen, zu prüfen, ob der Administrationsagent installiert ist und gestartet wurde.

Fehler bei Anmeldung am Administrationsagenten

Sollte dieser Fehler auftreten, dann folgen Sie den Empfehlungen zum Beheben von Fehlern dieser Gruppe. Sollte sich der Fehler wiederholen, dann erstellen Sie eine ausführliche Berichtsdatei (Routing) des Updates und des Administrationsagenten auf diesem Computer und verwenden Sie das Webformular, um die Berichtsdateien mit einer Fehlerbeschreibung an den Technischen Support-Service zu senden.

Verbindungsversuch ist fehlgeschlagen. Der Administrationsserver ist überlastet und kann die Anfrage nicht verarbeiten

Es wird empfohlen, in diesem Fall den Updateversuch später zu wiederholen.

Es kann keine Verbindung mit dem Administrationsserver/ Haupt-Administrationsserver/ Administrationsagenten hergestellt werden, physikalischer Fehler/ unbekannter Fehler

Wenn Fehler dieser Art auftreten, wird empfohlen, den Updateversuch später zu wiederholen. Sollte der Versuch erfolglos sein, wenden Sie sich an den technischen Kundendienst.

Eine Datei kann nicht vom Administrationsserver empfangen werden, ungültiges Transportargument

Wenn dieser Fehler erneut auftreten sollte, wenden Sie sich an den technischen Kundendienst.

Fehler beim Empfang einer Datei vom Administrationsserver

Wenn Fehler dieser Art auftreten, wird empfohlen, den Updateversuch später zu wiederholen. Sollte der Versuch erfolglos sein, wenden Sie sich an den technischen Kundendienst.

SONSTIGE CODES

Zu dieser Gruppe zählen Fehler, die zu keiner der oben genannten Gruppen gehören.

Es fehlen Dateien für die Rollback-Operation

Dieser Fehler tritt auf, wenn ein Update rückgängig gemacht wurde und ein erneuter Versuch zum Rollback erfolgte, ohne dazwischen ein Update vorzunehmen. Es ist nicht möglich, die Rückkehroperation auszuführen, bevor kein erfolgreiches Update erfolgte, durch das eine Sicherungskopie der Updatedateien angelegt wird.

PROGRAMMPARAMETER ANPASSEN

Das Programmkonfigurationsfenster dient dem schnellen Zugriff auf die wichtigsten Einstellungen von Kaspersky Anti-Virus 6.0.

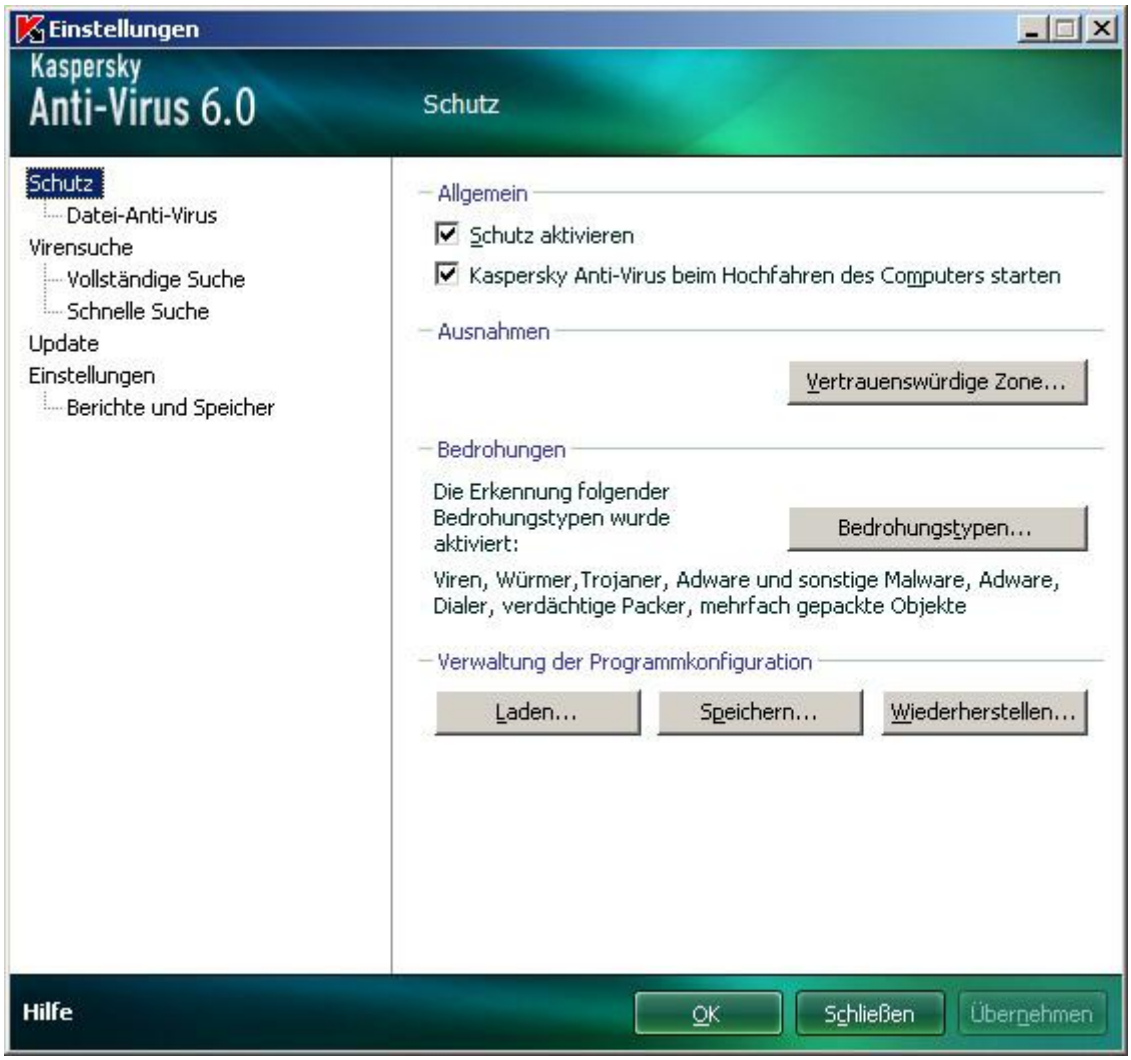


Abbildung 9. Programmkonfigurationsfenster

Das Fenster besteht aus zwei Teilen:

- Die linke Fensterseite bietet Zugriff auf Datei-Anti-Virus, auf Untersuchungs- und Updateaufgaben, u.a.
- Die rechte Seite des Fensters enthält eine Liste von Parametern für die auf der linken Seite ausgewählte Komponente, Aufgabe usw.

Zum Öffnen des Fensters gibt es folgende Möglichkeiten:

- aus dem Programmhauptfenster. Klicken Sie dazu im oberen Bereich des Hauptfensters auf die Schaltfläche **Einstellungen**.

- aus dem Kontextmenü. Wählen Sie dazu im Kontextmenü des Programms den Punkt **Einstellungen** aus.

Abbildung 10. Kontextmenü

IN DIESEM ABSCHNITT

SCHUTZ

Im Fenster **Schutz** können Sie folgende Zusatzfunktionen von Kaspersky Anti-Virus verwenden:

- Schutz deaktivieren / aktivieren (s. S. 76).
- Anwendung beim Hochfahren des Betriebssystems starten (s. S. 77).
- Auswahl der Kategorien der erkennbaren Bedrohungen (s. S. 77).
- Anlegen der vertrauenswürdigen Zone (s. S. 78):
  - Erstellen einer Ausnahmeregel (s. S. 78).
  - Erstellen einer Liste der vertrauenswürdigen Anwendungen (s. S. 81).
  - Export / Import von Komponenten der vertrauenswürdigen Zone (s. S. 81).
- Export / Import von Parametern für die Programmfunktion (s. S. 82).
- Wiederherstellen der standardmäßigen Parameter für die Programmfunktion (s. S. 82).

SCHUTZ DES COMPUTERS DEAKTIVIEREN / AKTIVIEREN

Kaspersky Anti-Virus wird in der Grundeinstellung automatisch beim Start des Betriebssystems gestartet und schützt Ihren Computer während der gesamten Sitzung. Datei-Anti-Virus ist aktiv.

Sie können den durch Datei-Anti-Virus gewährleisteten Schutz vollständig deaktivieren.

Kaspersky Lab empfiehlt ausdrücklich, den Schutz **nicht zu deaktivieren**, weil dies zur Infektion des Servers und zu Datenverlust führen kann.

Durch das Deaktivieren des Schutzes wird Datei-Anti-Virus beendet. Das Deaktivieren der Komponente übt keinen Einfluss auf die von Kaspersky Anti-Virus ausgeführten Untersuchungs- und Updateaufgaben aus.

Gehen Sie folgendermaßen vor, um den Schutz vollständig auszuschalten:

1. Öffnen Sie das Programmkonfigurationsfenster.
2. Wählen Sie auf der linken Fensterseite den Abschnitt **Schutz**.
3. Deaktivieren Sie das Kontrollkästchen **Schutz aktivieren**.

ANWENDUNG BEIM HOCHFAHREN DES BETRIEBSSYSTEMS STARTEN.

Sollte es erforderlich sein, die Kaspersky Anti-Virus vollständig zu beenden, dann wählen Sie den Punkt **Beenden** im Kontextmenü des Programms. Dadurch wird das Programm aus dem Arbeitsspeicher entfernt. Das bedeutet, dass der Computer dann im ungeschützten Modus arbeitet.

Der Computerschutz kann erneut aktiviert werden, indem das Programm aus dem **Startmenü** → **Programme** → **Kaspersky Anti-Virus 6.0** → **Kaspersky Anti-Virus 6.0** gestartet wird.

Außerdem kann der Schutz nach dem Neustart des Betriebssystems automatisch gestartet werden.

Gehen Sie folgendermaßen vor, um den Modus zu aktivieren, in dem die Anwendung beim Hochfahren des Betriebssystems gestartet wird:

1. Öffnen Sie das Programmkonfigurationsfenster.
2. Wählen Sie auf der linken Fensterseite den Abschnitt **Schutz**.
3. Aktivieren Sie das Kontrollkästchen **Kaspersky Anti-Virus beim Hochfahren des Computers starten**.

AUSWAHL DER KATEGORIEN DER ERKENNBAREN BEDROHUNGEN

Das Programm Kaspersky Anti-Virus bietet Ihnen Schutz vor verschiedenen Arten schädlicher Programme. Unabhängig von den festgelegten Parametern untersucht und neutralisiert das Programm immer Viren und trojanische Programme. Diese Programme können Ihrem Computer ernsthaften Schaden zufügen. Um die Sicherheit des Computers zu erhöhen, können Sie die Liste der erkennbaren Bedrohungen erweitern. Aktivieren Sie dazu die Kontrolle für unterschiedliche Arten potentiell gefährlicher Programme.

Gehen Sie folgendermaßen vor, um die Kategorien erkennbare Bedrohungen auszuwählen:

1. Öffnen Sie das Programmkonfigurationsfenster.
2. Wählen Sie auf der linken Fensterseite den Abschnitt **Schutz**.
3. Klicken Sie im Block **Bedrohungen** auf die Schaltfläche **Bedrohungstypen**.
4. Aktivieren Sie im folgenden Fenster **Bedrohungstypen** die Kontrollkästchen der Bedrohungskategorien, vor denen Sie Ihren Computer schützen möchten.

ANLEGEN DER VERTRAUENSWÜRDIGEN ZONE

Die *vertrauenswürdige Zone* ist eine benutzerdefinierte Liste von Objekten, die von Kaspersky Anti-Virus nicht kontrolliert werden. Mit anderen Worten ist dies eine Auswahl von Ausnahmen für den Schutz des Programms.

Die vertrauenswürdige Zone wird vom Benutzer unter Berücksichtigung der Besonderheiten von Objekten, mit denen er arbeitet, sowie von Programmen, die auf seinem Computer installiert sind, aufgebaut. Das Anlegen einer solchen Liste mit Ausnahmen kann beispielsweise erforderlich sein, wenn Kaspersky Anti-Virus den Zugriff auf ein bestimmtes Objekt oder Programm blockiert, Sie aber sicher sind, dass dieses Objekt bzw. Programm absolut unschädlich ist.

Von der Untersuchung können ausgeschlossen werden: Dateien eines bestimmten Formats, Dateien nach Maske, bestimmte Bereiche (beispielsweise ein Ordner oder Programm) sowie Programmprozesse oder Objekte gemäß der Klassifikation der Viren-Enzyklopädie (Status, der einem Objekt bei der Untersuchung durch Kaspersky Anti-Virus zugewiesen wurde).

Ein ausgeschlossenes Objekt unterliegt nicht der Untersuchung, wenn das Laufwerk oder der Ordner untersucht wird, auf dem es sich befindet. Wird allerdings ein konkretes Objekt zur Untersuchung ausgewählt, dann wird die Ausnahmeregel ignoriert.

➡ *Gehen Sie folgendermaßen vor, um eine Liste von Ausnahmen für den Schutz zu erstellen:*

1. Öffnen Sie das Programmkonfigurationsfenster.
2. Wählen Sie auf der linken Fensterseite den Abschnitt **Schutz**.
3. Klicken Sie im Block **Ausnahmen** auf die Schaltfläche **Vertrauenswürdige Zone**.
4. Passen Sie im folgenden Fenster die Ausnahmeregeln für die Objekte an (s. S. 78) und legen Sie die Liste der vertrauenswürdigen Anwendungen (s. S. 81) an.

SIEHE AUCH

ERSTELLEN EINER AUSNAHMEREGEL

Eine Ausnahmeregel ist eine Kombination von Bedingungen, bei deren Vorhandensein ein Objekt nicht von Kaspersky Anti-Virus untersucht wird.

Von der Untersuchung können ausgeschlossen werden: Dateien eines bestimmten Formats, Dateien nach Maske, bestimmte Bereiche (beispielsweise ein Ordner oder Programm) sowie Programmprozesse oder Objekte gemäß der Klassifikation der Viren-Enzyklopädie.

Ein Bedrohungstyp ist ein Status, der einem Objekt von dem Programm Kaspersky Anti-Virus bei der Untersuchung zugewiesen wird. Der Bedrohungstyp beruht auf einer Klassifikation schädlicher und potentiell gefährlicher Programme, die in der Viren-Enzyklopädie von Kaspersky Lab enthalten ist.

Ein potentiell gefährliches Programm besitzt keine schädliche Funktion, kann aber von einem Schadprogramm als Hilfskomponente benutzt werden, weil es Schwachstellen und Fehler enthält. Zu dieser Kategorie gehören beispielsweise Programme zur Remote-Verwaltung, IRC-Clients, FTP-Server, alle Hilfsprogramme zum Beenden von Prozessen und

zum Verstecken ihrer Arbeit, Tastaturspione, Programme zur Kennwortermittlung, Programme zur automatischen Einwahl auf kostenpflichtige Seiten usw. Solche Software wird nicht als Virus klassifiziert (not-a-virus), lässt sich aber beispielsweise in folgende Typen unterteilen: Adware, Joke, Riskware u.a. (ausführliche Informationen über potentiell gefährliche Programme, die von Kaspersky Anti-Virus entdeckt werden können, finden Sie in der Viren-Enzyklopädie auf der Seite www.viruslist.com/de (http://www.viruslist.com/de/viruses/encyclopedia)). Derartige Programme können aufgrund der Untersuchung gesperrt werden. Da bestimmte Programme dieser Kategorie von vielen Benutzern verwendet werden, besteht die Möglichkeit, sie von der Untersuchung auszuschließen. Dazu muss zur vertrauenswürdigen Zone der Name oder eine Maske der Bedrohung gemäß der Klassifikation der Viren-Enzyklopädie hinzugefügt werden.

Es kann beispielsweise sein, dass Sie häufig mit dem Programm Remote Administrator arbeiten. Dabei handelt es sich um ein System, das dem Remote-Zugriff dient und die Arbeit auf einem Remote-Computer erlaubt. Diese Anwendungsaktivität wird von Kaspersky Anti-Virus als potentiell gefährlich eingestuft und kann blockiert werden. Um zu verhindern, dass die Anwendung blockiert wird, muss eine Ausschlussregel mit der Klassifikation Remote Admin erstellt werden.

Beim Hinzufügen einer Ausnahme wird eine Regel erstellt, die anschließend von Datei-Anti-Virus und bei der Ausführung von Untersuchungsaufgaben verwendet werden kann.

Gehen Sie folgendermaßen vor, um eine Ausnahmeregel zu erstellen:

1. Öffnen Sie das Programmkonfigurationsfenster.
2. Wählen Sie auf der linken Fensterseite den Abschnitt **Schutz**.
3. Klicken Sie im Block **Ausnahmen** auf die Schaltfläche **Vertrauenswürdige Zone**.
4. Klicken Sie im folgenden Fenster auf der Registerkarte **Regeln für Ausnahmen** auf die Schaltfläche **Hinzufügen**.
5. Legen Sie im folgenden Fenster **Ausnahmeregel** im Block **Einstellungen** den Typ der Ausnahme fest. Geben Sie dann im Block **Beschreibung** Werte für die gewählten Ausnahmetypen an und legen Sie fest, für welche Komponenten von Kaspersky Anti-Virus die neue Regel bei der Arbeit verwendet werden soll.

Gehen Sie folgendermaßen vor, um eine Ausnahmeregel vom Berichtsfenster aus zu erstellen:

1. Wählen Sie im Bericht das Objekt aus, das Sie zu den Ausnahmen hinzufügen möchten.
2. Wählen Sie im Kontextmenü für dieses Objekt den Punkt **Zur vertrauenswürdigen Zone hinzufügen**.
3. Überprüfen Sie im folgenden Fenster **Ausnahmeregel**, ob alle Parameter der Ausnahmeregel korrekt sind. Die Felder mit dem Objektnamen und dem zugewiesenen Bedrohungstyp werden automatisch ausgefüllt, wozu Informationen aus dem Bericht dienen. Klicken Sie auf die Schaltfläche **OK**, um die Regel zu erstellen.

ZULÄSSIGE AUSSCHLUSSMASKEN FÜR DATEIEN

Hier werden Beispiele für zulässige Masken genannt, die Sie beim Erstellen der Liste auszuschließender Dateien verwenden können:

1. Masken ohne Dateipfad:
   - ***.exe** – alle Dateien mit der Endung *exe*;
   - ***.ex?** – alle Dateien mit der Endung *ex?*, wobei anstelle von *?* ein beliebiges Zeichen stehen kann.
   - **test** – alle Dateien mit dem Namen *test*
2. Masken mit absolutem Dateipfad:
   - **C:\dir*.*** oder **C:\dir*** oder **C:\dir** - alle Dateien im Ordner *C:\dir*;
   - **C:\dir*.exe** – alle Dateien mit der Endung *exe* im Ordner C:\dir\;

- **C:\dir*.ex?** – alle Dateien mit der Endung *ex?* im Ordner *C:\dir*, wobei anstelle von *?* ein beliebiges Zeichen stehen kann.

- **C:\dir\test** – nur die Datei *C:\dir\test*.

  Damit auch die Dateien in allen untergeordneten Ordnern des gewählten Ordners von der Untersuchung ausgeschlossen werden, aktivieren Sie beim Erstellen der Maske das Kontrollkästchen ☑ **Unterordner einschließen**.

3. Masken mit Dateipfad:

   - **dir*.*** oder **dir*** oder **dir** - alle Dateien in allen Ordnern von *dir*;

   - **dir\test** – alle Dateien mit dem Namen *test* in den Ordnern von *dir*;

   - **dir*.exe** – alle Dateien mit der Endung *exe* in allen Ordnern *dir*;

   - **dir*.ex?** – alle Dateien mit der Endung *ex?* in allen Ordnern von *dir*, wobei anstelle von *?* ein beliebiges Zeichen stehen kann.

     Damit auch die Dateien in allen untergeordneten Ordnern des gewählten Ordners von der Untersuchung ausgeschlossen werden, aktivieren Sie beim Erstellen der Maske das Kontrollkästchen ☑ **Unterordner einschließen**.

Die Verwendung der Ausnahmemaske *.* oder * ist nur zulässig, wenn die auszuschließende Bedrohung gemäß der Viren-Enzyklopädie klassifiziert wird. In diesem Fall wird die Bedrohung nicht in allen Objekten gefunden werden. Wenn diese Masken ohne Angabe einer Klassifikation verwendet werden, entspricht dies dem Deaktivieren des Schutzes. Außerdem wird davor gewarnt, den Pfad eines virtuellen Laufwerks, das auf Basis eines Dateisystemordners mit dem Befehl subst erstellt wurde, oder den Pfad eines Laufwerks, das der Mirror eines Netzwerkordners ist, als Ausnahme auszuwählen. Es kann sein, dass unterschiedliche Benutzer eines Computers unterschiedliche Ressourcen mit einem identischen Laufwerksnamen bezeichnen, was beim Auslösen von Ausnahmeregeln unvermeidlich zu Fehlern führt.

SIEHE AUCH

Zulässige Ausschlussmasken gemäß der Klassifikation der Viren-Enzyklopädie 80

ZULÄSSIGE AUSSCHLUSSMASKEN GEMÄß DER KLASSIFIKATION DER VIREN-ENZYKLOPÄDIE

Wenn eine Bedrohung, die ein bestimmtes Verdikt nach der Klassifikation der Viren-Enzyklopädie besitzt, als Ausnahme hinzugefügt wird, können Sie angeben:

- den vollständigen Namen der Bedrohung, wie er in der Viren-Enzyklopädie auf der Seite www.viruslist.com/de (http://www.viruslist.com/de/viruses/encyclopedia) genannt wird (beispielsweise **not-a-virus:RiskWare.RemoteAdmin.RA.311** oder **Flooder.Win32.Fuxx**).

- den Namen der Bedrohung als Maske, beispielsweise:

  - **not-a-virus*** – Legale, aber potentiell gefährliche Programme sowie Scherzprogramme von der Untersuchung ausschließen.

  - ***Riskware.*** – Alle potentiell gefährlichen Programme des Typs Riskware von der Untersuchung ausschließen.

  - ***RemoteAdmin.*** – Alle Versionen von Programmen zur Fernverwaltung von der Untersuchung ausschließen.

SIEHE AUCH

ERSTELLEN EINER LISTE DER VERTRAUENSWÜRDIGEN ANWENDUNGEN.

Sie können eine Liste mit vertrauenswürdigen Programmen erstellen, deren Aktivität nicht kontrolliert wird. Dies bezieht sich auch auf verdächtige Aktivität, Datei- und Netzwerkaktivität sowie Zugriff auf die Systemregistrierung.

Sie halten beispielsweise die Objekte, die von dem standardmäßigen Microsoft Windows-Programm **Editor** verwendet werden, für ungefährlich und deren Untersuchung im Schutz nicht für erforderlich. Das bedeutet, dass Sie diesem Programm vertrauen. Um die Objekte, die von diesem Prozess benutzt werden, von der Untersuchung auszuschließen, fügen Sie das Programm **Editor** zur Liste der vertrauenswürdigen Programme hinzu. Trotzdem werden aber die ausführbare Datei und der Prozess einer vertrauenswürdigen Anwendung weiterhin auf Viren untersucht. Um ein Programm vollständig von der Untersuchung auszuschließen, müssen die Ausnahmeregeln verwendet werden.

Einige Aktionen, die als gefährlich klassifiziert werden, sind im Rahmen der Funktionalität bestimmter Programme normal. Beispielsweise ist das Abfangen eines Texts, den Sie über die Tastatur eingeben, für Programme zum automatischen Umschalten der Tastaturbelegung (Punto Switcher u.ä.) eine normale Aktion. Um die Besonderheit solcher Programme zu berücksichtigen und die Kontrolle ihrer Aktivität auszuschalten, empfehlen wir, sie in die Liste der vertrauenswürdigen Anwendungen aufzunehmen.

Das Ausschließen vertrauenswürdiger Anwendungen aus der Untersuchung erlaubt es außerdem, mögliche Kompatibilitätsprobleme von Kaspersky Anti-Virus mit anderen Anwendungen zu lösen (wenn beispielsweise der Netzwerkverkehr von einem anderen Computer bereits von einer Antiviren-Anwendung untersucht wurde). Außerdem lässt sich auf diese Weise die Leistungsfähigkeit des Computers erhöhen, was insbesondere bei der Verwendung von Serveranwendungen wichtig ist.

Kaspersky Anti-Virus untersucht standardmäßig alle Objekte, die von einem beliebigen Programmprozess geöffnet, gestartet oder gespeichert werden sollen, und kontrolliert die Aktivität aller Programme und den von ihnen erzeugten Netzwerkverkehr.

Gehen Sie folgendermaßen vor, um ein Programm zur Liste der vertrauenswürdigen Programme hinzuzufügen:

1. Öffnen Sie das Programmkonfigurationsfenster.
2. Wählen Sie auf der linken Fensterseite den Abschnitt **Schutz**.
3. Klicken Sie im Block **Ausnahmen** auf die Schaltfläche **Vertrauenswürdige Zone**.
4. Klicken Sie im folgenden Fenster auf der Registerkart .**Vertrauenswürdige Anwendungen** auf die Schaltfläche **Hinzufügen**.
5. Wählen Sie im folgenden Fenster **Vertrauenswürdige Anwendung** eine Anwendung aus. Verwenden Sie dazu die Schaltfläche **Durchsuchen**. Dadurch öffnet sich ein Kontextmenü, in dem Sie mit dem Punkt **Durchsuchen** in das Standardfenster zur Dateiauswahl gelangen, um den Pfad der ausführbaren Datei anzugeben, oder mit dem Punkt **Anwendungen** zur Liste der momentan aktiven Anwendungen wechseln können, um die gewünschte auszuwählen. Legen Sie die entsprechenden Parameter für die ausgewählte Anwendung fest.

EXPORT / IMPORT VON KOMPONENTEN DER VERTRAUENSWÜRDIGEN ZONE

Die Funktionen zum Export und Import dienen dazu, vorhandene Ausnahmeregeln und Listen mit vertrauenswürdigen Anwendungen auf andere Computer zu übertragen.

Gehen Sie folgendermaßen vor, um vorhandene Ausnahmeregeln zu kopieren:

1. Öffnen Sie das Programmkonfigurationsfenster.
2. Wählen Sie auf der linken Fensterseite den Abschnitt **Schutz**.

3. Klicken Sie im Block **Ausnahmen** auf die Schaltfläche **Vertrauenswürdige Zone**.

4. Verwenden Sie im folgenden Fenster auf der Registerkarte **Regeln für Ausnahmen** die Schaltflächen **Export** und **Import**, um Regeln zu kopieren.

Gehen Sie folgendermaßen vor, um eine Liste mit vertrauenswürdigen Anwendungen zu kopieren:

1. Öffnen Sie das Programmkonfigurationsfenster.

2. Wählen Sie auf der linken Fensterseite den Abschnitt **Schutz**.

3. Klicken Sie im Block **Ausnahmen** auf die Schaltfläche **Vertrauenswürdige Zone**.

4. Verwenden Sie im folgenden Fenster auf der Registerkarte **Vertrauenswürdige Anwendungen** die Schaltflächen **Export** und **Import**, um die Liste zu kopieren.

EXPORT / IMPORT DER EINSTELLUNGEN VON KASPERSKY ANTI-VIRUS

Kaspersky Anti-Virus bietet Ihnen die Möglichkeit zum Exportieren und Importieren seiner Programmeinstellungen.

Diese Option kann beispielsweise von Nutzen sein, wenn Sie das Programm auf Ihrem PC zuhause und im Büro installiert haben. Sie können das Programm entsprechend konfigurieren, die Einstellungen auf einer Diskette speichern und mit Hilfe der Importfunktion schnell auf Ihren Computer im Büro laden. Die Einstellungen werden in einer speziellen Konfigurationsdatei gespeichert.

Gehen Sie folgendermaßen vor, um die aktuellen Programmparameter zu exportieren:

1. Öffnen Sie das Programmkonfigurationsfenster.

2. Wählen Sie auf der linken Fensterseite den Abschnitt **Schutz**.

3. Klicken Sie im Block **Verwaltung der Programmkonfiguration** auf die Schaltfläche **Speichern**.

4. Geben Sie im folgenden Fenster einen Namen für die Konfigurationsdatei an und wählen Sie einen Speicherort dafür.

Gehen Sie folgendermaßen vor, um die Funktionsparameter aus einer Konfigurationsdatei zu importieren:

1. Öffnen Sie das Programmkonfigurationsfenster.

2. Wählen Sie auf der linken Fensterseite den Abschnitt **Schutz**.

3. Klicken Sie im Block **Verwaltung der Programmkonfiguration** auf die Schaltfläche **Laden**.

4. Wählen Sie im folgenden Fenster eine Datei aus, aus der Sie die Parameter für Kaspersky Anti-Virus importieren möchten.

WIEDERHERSTELLEN DER STANDARDEINSTELLUNGEN

Sie können jederzeit zu den empfohlenen Einstellungen für Kaspersky Anti-Virus zurückkehren. Diese gelten als optimal und werden von Kaspersky Lab empfohlen. Die Wiederherstellung der Einstellungen erfolgt mit Hilfe des Konfigurationsassistenten.

Im folgenden Fenster können Sie festlegen, welche Parameter bei der Wiederherstellung der empfohlenen Sicherheitsstufe beibehalten werden sollen.

Nach dem Abschluss des Assistenten wird für Datei-Anti-Virus die Sicherheitsstufe **Empfohlen** eingestellt, wobei die Parameter berücksichtigt werden, die Sie beim Wiederherstellen zum Speichern ausgewählt haben. Zusätzlich werden die Einstellungen übernommen, die Sie während der Arbeit des Assistenten vorgenommen haben.

Gehen Sie folgendermaßen vor, um die Schutzeinstellungen wiederherzustellen:

1. Öffnen Sie das Programmkonfigurationsfenster.
2. Wählen Sie auf der linken Fensterseite den Abschnitt **Schutz**.
3. Klicken Sie im Block **Verwaltung der Programmkonfigurationn** auf die Schaltfläche **Wiederherstellen**.
4. Aktivieren Sie im folgenden Fenster die Kontrollkästchen der Parameter, die gespeichert werden sollen. Klicken Sie auf **Weiter**. Der Konfigurationsassistent wird gestartet. Folgen Sie den Anweisungen.

DATEI-ANTI-VIRUS

Dieses Fenster enthält die Parameter der Komponente **Datei-Anti-Virus** (s. Abschnitt "Antiviren-Schutz für das Dateisystem des Computers" auf S. 39). Mit Hilfe der Parameterwerte können Sie:

- Sicherheitsstufe ändern (s. S. 41).
- die Aktion ändern, die auf gefundene Objekte angewendet wird (s. S. 41).
- den Schutzbereich festlegen (s. S. 43).
- Untersuchung optimieren (s. S. 44).
- die Untersuchung zusammengesetzter Dateien anpassen (s. S. 44).
- Untersuchungsmodus ändern (s. S. 46).
- heuristische Analyse verwenden (s. S. 44).
- die Arbeit der Komponente anhalten (s. S. 47).
- Untersuchungstechnologien wählen (s. S. 46).
- die Standardparameter wiederherstellen (s. S. 48), falls sie geändert wurden.

Gehen Sie folgendermaßen vor, um zu den Einstellungen für Datei-Anti-Virus zu gelangen:

1. Öffnen Sie das Programmkonfigurationsfenster.
2. Wählen Sie auf der linken Fensterseite den Abschnitt **Datei-Anti-Virus**.
3. Wählen Sie auf der rechten Fensterseite die Sicherheitsstufe und die Reaktion der Komponente auf die Bedrohung aus. Klicken Sie auf die Schaltfläche **Einstellungen**, um andere Parameter von Datei-Anti-Virus anzupassen.

VIRENSUCHE

Auf welche Weise die Untersuchung von Objekten auf Ihrem Computer erfolgt, wird durch eine Auswahl von Parametern bestimmt, die für jede Aufgabe festgelegt werden.

Die Spezialisten von Kaspersky Lab haben mehrere Aufgaben für die Virensuche vorgesehen. Dazu gehören folgende:

Virensuche

Untersuchung von Objekten, die der Benutzer festlegt. Sie können ein beliebiges Objekt des Dateisystems auf dem Computer untersuchen.

Vollständige Suche

Ausführliche Untersuchung des Systems. Standardmäßig werden folgende Objekte untersucht: Systemspeicher, Objekte, die beim Systemstart gestartet werden, Systemwiederherstellung, Mail-Datenbanken, Festplatten, Wechseldatenträger und Netzlaufwerke.

Schnelle Suche

Virenuntersuchung der Objekte, die beim Start des Betriebssystems geladen werden.

Im Konfigurationsfenster können Sie für jede Aufgabe:

- die Sicherheitsstufe (s. S. 53) wählen, auf deren Basis die Aufgabe ausgeführt werden soll.
- die Aktion (s. S. 53) wählen, die vom Programm beim Fund eines infizierten bzw. möglicherweise infizierten Objekts angewandt wird.
- einen Zeitplan (s. S. 59) für den automatischen Aufgabenstart erstellen.
- die Typen der Dateien (s. S. 55), die der Virenanalyse unterzogen werden, festlegen.
- Parameter für die Untersuchung zusammengesetzter Dateien (s. S. 56) festlegen.
- Methoden und Technologien für die Untersuchung auswählen (s. S. 57).
- einheitliche Untersuchungsparameter für alle Aufgaben (s. S. 61) festlegen.

Gehen Sie folgendermaßen vor, um die Aufgabenparameter anzupassen:

1. Öffnen Sie das Programmhauptfenster.
2. Wählen Sie auf der linken Fensterseite den Abschnitt **Virensuche** (**Vollständige Suche**, **Schnelle Suche**).
3. Wählen Sie auf der rechten Fensterseite die Sicherheitsstufe und die Reaktion auf die Bedrohung aus und passen Sie den Startmodus an. Klicken Sie auf die Schaltfläche **Einstellungen**, um andere Parameter der Aufgabe anzupassen. Um die standardmäßigen Parameter wiederherzustellen, klicken Sie auf die Schaltfläche **Grundeinstellung**.

UPDATE

Das Update von Kaspersky Anti-Virus wird nach den Parametern ausgeführt, die festlegen:

- von welcher Ressource (s. S. 65) der Download und die Installation der Programm-Updates erfolgen.
- in welchem Modus (s. S. 68) der Updateprozess des Programms gestartet wird und welche Elemente aktualisiert werden sollen.
- wie oft die Aktualisierung erfolgen soll, falls der Start nach Zeitplan (s. S. 67) festgelegt wird.
- unter welchem Benutzerkonto (s. S. 67) der Start des Updates erfolgt.
- ob das Kopieren der heruntergeladenen Updates in eine lokale Quelle ausgeführt werden soll (s. S. 69).
- Verwendung eines Proxyservers (s. S. 66).

Gehen Sie folgendermaßen vor, um zur Konfiguration der Updateparameter zu wechseln:

1. Öffnen Sie das Programmkonfigurationsfenster.
2. Wählen Sie auf der linken Fensterseite den Abschnitt **Update**.
3. Wählen Sie auf der rechten Fensterseite den erforderlichen Startmodus. Klicken Sie auf die Schaltfläche **Einstellungen**, um andere Parameter der Aufgabe anzupassen.

PARAMETER

Im Fenster **Einstellungen** können Sie folgende Zusatzfunktionen von Kaspersky Anti-Virus verwenden:

- Selbstschutz für das Programm (s. S. 85).
- Kontrolle des Zugriffs auf das Programm (s. S. 86).
- Größenbeschränkung für iSwift-Dateien (s. S. 86).
- Leistung des Servers bei Verwendung einer Multiprozessor-Konfiguration (s. S. 87).
- Benachrichtigungen über die Ereignisse von Kaspersky Anti-Virus (s. S. 87):
  - Auswahl des Ereignistyps und der Methode zum Senden von Benachrichtigungen (s. S. 88).
  - Anpassen des Sendens von Benachrichtigungen per E-Mail (s. S. 89).
  - Parameter des Ereignisberichts (s. S. 89).
- Aktive Elemente der Benutzeroberfläche (s. S. 89).

SELBSTSCHUTZ FÜR DAS PROGRAMM

Kaspersky Anti-Virus bietet dem Computer Sicherheit vor schädlichen Programmen und wird dadurch selbst zu einem Objekt von Schädlingen, die versuchen können, die Arbeit der Anwendung zu blockieren oder sie sogar vom Computer zu löschen.

Um die Stabilität des Sicherheitssystems für Ihren Computer zu gewährleisten, verfügt das Programm über Mechanismen zum Selbstschutz und zum Schutz vor externem Zugriff.

In 64-Bit-Betriebssystemen des Typs Microsoft Windows Server 2008 (ohne Service Packs) und Microsoft Windows Server 2003 erstreckt sich der Schutz vor Veränderungen und Löschen nur auf Programmdateien auf der Festplatte sowie auf Einträge in der Systemregistrierung.

Wenn der Schutz vor Fernsteuerung verwendet wird, ist es erforderlich, Programmen, die der Remote-Administration dienen (z.B. RemoteAdmin), den Zugriff auf die Anwendungssteuerung zu gewähren. Dazu werden diese Programme zur Liste der vertrauenswürdigen Programme hinzugefügt und der Parameter **Interaktion mit Programminterface zulassen** wird für sie aktiviert.

Gehen Sie folgendermaßen vor, um die Selbstschutzmechanismen für das Programm zu aktivieren:

1. Öffnen Sie das Programmkonfigurationsfenster.
2. Wählen Sie auf der linken Fensterseite ein Abschnitt **Einstellungen**.
3. Aktivieren Sie im Block **Selbstschutz** das Kontrollkästchen ☑ **Selbstschutz aktivieren**, damit der Mechanismus zum Schutz der Anwendung vor dem Verändern oder Löschen von eigenen Dateien auf der Festplatte, Prozessen im Arbeitsspeicher und Einträgen in der Systemregistrierung wirksam wird.

Aktivieren Sie im Block **Selbstschutz** das Kontrollkästchen **Option zur externen Steuerung des Systemdiensts deaktivieren**, um alle Versuche zur Fernsteuerung eines Anwendungsdiensts zu blockieren.

Wird versucht, eine der oben genannten Aktionen auszuführen, dann erscheint eine Meldung über dem Programmsymbol im Infobereich der Taskleiste (falls der Benachrichtigungsdienst nicht vom Benutzer deaktiviert wurde).

KONTROLLE DES ZUGRIFFS AUF DAS PROGRAMM

Ein PC kann von verschiedenen Benutzern verwendet werden, deren Fertigkeiten im Umgang mit Computern möglicherweise nicht ausreichend sind. Der ungehinderte Zugriff auf das Programm und dessen Einstellungen kann das Sicherheitsniveau des Computers stark einschränken.

Um die Sicherheit des Computers zu erhöhen, verwenden Sie ein Kennwort für den Zugriff auf Kaspersky Anti-Virus. Sie können entweder alle Operationen blockieren (unter Ausnahme der Arbeit mit Meldungen über den Fund gefährlicher Objekte) oder das Ausführen folgender Aktionen untersagen:

- Programmparameter ändern.
- Programm beenden.
- Datei-Anti-Virus oder Untersuchungsaufgaben deaktivieren.
- Richtlinie deaktivieren (wenn die Anwendung über Kaspersky Administration Kit verwaltet wird).
- Deinstallation der Anwendung.

Jede der oben genannten Aktionen führt zu einer Verringerung des Schutzniveaus Ihres Computers. Deshalb sollten Sie festlegen, welche Benutzer Ihres Computers berechtigt sein sollen, diese Aktionen auszuführen.

Gehen Sie folgendermaßen vor, um den Zugriff auf das Programm durch ein Kennwort zu schützen:

1. Öffnen Sie das Programmkonfigurationsfenster.
2. Wählen Sie auf der linken Fensterseite ein Abschnitt **Einstellungen**.
3. Aktivieren Sie im Block **Kennwortschutz** das Kontrollkästchen **Kennwortschutz aktivieren** und klicken Sie auf die Schaltfläche **Einstellungen**.
4. Legen Sie im folgenden Fenster **Kennwortschutz** ein Kennwort fest und wählen Sie den Bereich, für den die Zugriffsbeschränkung gelten soll. Wenn künftig ein beliebiger Benutzer auf Ihrem Computer versucht, die von Ihnen festgelegten Aktionen auszuführen, wird das Programm stets nach dem Kennwort fragen.

GRÖßENBESCHRÄNKUNG FÜR ISWIFT-DATEIEN

iSwift-Dateien – Dateien, die Informationen über bereits auf Viren untersuchte Objekte eines NTFS-Dateisystems enthalten (iSwift-Technologie). Der Einsatz solcher Dateien erlaubt es, die Objektuntersuchung zu beschleunigen, weil Kaspersky Anti-Virus nur jene Objekte untersucht, die seit dem letzten Scan verändert wurden. Die iSwift-Dateien werden im Lauf der Zeit sehr umfangreich. Es wird empfohlen, eine Größenbeschränkung für diese Dateien festzulegen. Wenn sie den Grenzwert erreicht, wird eine iSwift-Datei bereinigt.

Gehen Sie folgendermaßen vor, um die Größe der iSwift-Dateien zu beschränken:

1. Öffnen Sie das Programmkonfigurationsfenster.
2. Wählen Sie auf der linken Fensterseite ein Abschnitt **Einstellungen**.
3. Aktivieren Sie im Block **Ressourcen** das Kontrollkästchen **iSwift-Datenbank leeren, wenn größer als** und geben Sie daneben die Größe der Datenbank in MB an.

MULTIPROZESSOR-KONFIGURATION DES SERVERS

Bei Verwendung einer Multiprozessor-Konfiguration des Servers, können Sie die Serverleistung in folgender Hinsicht anpassen:

- Festlegen der Anzahl von Exemplaren des Antiviren-Kerns, die beim Start von Kaspersky Anti-Virus auf dem Server geladen werden. Dieser Wert bestimmt die Anzahl der Antiviren-Prozesse, die parallel auf dem Server laufen.

  Je größer die Anzahl der gestarteten Kopien des Antiviren-Kerns, desto schneller wird die Antiviren-Verarbeitung der Objekte ausgeführt. Allerdings wirkt sich dies auf die Gesamtleistung des Servers aus. Bei unzureichender Größe des Arbeitsspeichers und einer hohen Anzahl gestarteter Kopien des Antiviren-Kerns können bei der Arbeit von Datei-Anti-Virus Störungen auftreten.

  Wenn gleichzeitig mehrere Antiviren-Prozesse laufen, bleibt der kontinuierliche Serverschutz auch dann aufrechterhalten, wenn beispielsweise bei der Arbeit eines Kerns eine Störung auftreten sollte.

- Belastung des Servers regulieren: Beispielsweise kann ein Teil der Prozessoren für die Antiviren-Verarbeitung von Objekten, ein anderer Teil für direkte Serveraufgaben vorgesehen werden.

  Kaspersky Lab empfiehlt, bei der Arbeit auf einem Multiprozessoren-Server mindestens einen Prozessor für die Serveraufgaben zu reservieren.

Gehen Sie folgendermaßen vor, um die Anzahl der Exemplare des Antiviren-Kerns festzulegen:

1. Öffnen Sie das Programmkonfigurationsfenster.
2. Wählen Sie auf der linken Fensterseite ein Abschnitt **Einstellungen**.
3. Klicken Sie im Block **Leistung** auf die Schaltfläche **Details**.
4. Legen Sie im folgenden Fenster **Multiprozessor-Konfiguration** im Block **Einstellungen** die Anzahl der Kopien für den Antiviren-Kern fest.

Gehen Sie folgendermaßen vor, um die Auslastung des Servers auszugleichen:

1. Öffnen Sie das Programmkonfigurationsfenster.
2. Wählen Sie auf der linken Fensterseite ein Abschnitt Einstellungen.
3. Klicken Sie im Block Leistung auf die Schaltfläche Details.
4. Deaktivieren Sie im folgenden Fenster **Multiprozessor-Konfiguration** im Block **Zu verwendende Prozessoren** die Kontrollkästchen für jene Prozessoren, die direkt für Serveraufgaben dienen sollen.

BENACHRICHTIGUNGEN ÜBER DIE EREIGNISSE VON KASPERSKY ANTI-VIRUS

Bei der Arbeit von Kaspersky Anti-Virus treten unterschiedliche Ereignisse ein. Sie können informativen Charakter besitzen oder wichtige Informationen enthalten. Ein Ereignis kann beispielsweise über die erfolgreiche Aktualisierung des Programms informieren oder einen Fehler bei der Arbeit einer bestimmten Komponente festhalten, der dringend behoben werden muss.

Um sich über die Ereignisse bei der Arbeit von Kaspersky Internet Security informieren zu lassen, verwenden Sie den Dienst für Benachrichtigungen.

Die Meldungen können durch eine der folgenden Methoden erfolgen:

- Popupmeldungen über dem Programmsymbol im Infobereich der Taskleiste

- Tonsignale.
- E-Mail-Nachrichten.
- Protokollieren von Informationen im Ereignisbericht.

Gehen Sie folgendermaßen vor, um den Dienst für Benachrichtigungen zu verwenden:

1. Öffnen Sie das Programmkonfigurationsfenster.
2. Wählen Sie auf der linken Fensterseite ein Abschnitt **Einstellungen**.
3. Aktivieren Sie im Block **Ansicht** das Kontrollkästchen **Ereignisbenachrichtigung aktivieren** und klicken Sie auf die Schaltfläche **Einstellungen**.
4. Legen Sie im folgenden Fenster **Benachrichtigungseinstellungen** die Ereignistypen für Kaspersky Anti-Virus fest, über deren Eintreten Sie benachrichtigt werden möchten. Geben Sie außerdem die Benachrichtigungsmethode an.

SIEHE AUCH

AUSWAHL DES EREIGNISTYPS UND DER METHODE ZUM SENDEN VON BENACHRICHTIGUNGEN

Bei der Arbeit von Kaspersky Anti-Virus treten Ereignisse der folgenden Typen auf:

- **Kritische Ereignisse** - Ereignisse mit kritischer Priorität. Es wird ausdrücklich empfohlen, sich über solche Ereignisse benachrichtigen zu lassen, weil sie auf Probleme bei der Arbeit des Programms oder auf Schwachstellen im Schutz Ihres Computers hinweisen. Beispiele: *Die Datenbanken sind stark veraltet* oder *Die Lizenzgültigkeit ist abgelaufen*.
- **Funktionsstörung** - Ereignisse, die zur Funktionsunfähigkeit des Programms führen. Beispiel: *Die Datenbanken fehlen oder sind beschädigt*.
- **Wichtige Ereignisse** – Ereignisse, die unbedingt beachtet werden müssen, weil Sie wichtige Situationen bei der Programmarbeit wiedergeben. Beispiele: *Die Datenbanken sind veraltet* oder *Die Lizenzgültigkeit endet bald*.
- **Informative Ereignisse** - Ereignisse mit informativem Charakter, die in der Regel keine wichtigen Informationen enthalten. Beispiel: *Objekt wurde nach Quarantäne verschoben*.

Gehen Sie folgendermaßen vor, um die für Benachrichtigungen relevanten Ereignisse und die entsprechenden Versandmethoden festzulegen:

1. Öffnen Sie das Programmkonfigurationsfenster.
2. Wählen Sie auf der linken Fensterseite ein Abschnitt **Einstellungen**.
3. Aktivieren Sie im Block **Ansicht** das Kontrollkästchen **Ereignisbenachrichtigung aktivieren** und klicken Sie auf die Schaltfläche **Einstellungen**.
4. Aktivieren Sie im folgenden Fenster **Benachrichtigungseinstellungen** die Kontrollkästchen für die Ereignisse, über die Sie benachrichtigt werden möchten, und für die entsprechenden Versandmethoden.

ANPASSEN DES SENDENS VON BENACHRICHTIGUNGEN PER E-MAIL

Nachdem Sie die Ereignisse (s. Abschnitt "Auswahl des Ereignistyps und der Methode zum Senden von Benachrichtigungen" auf S. 88) gewählt haben, über deren Eintreten Sie per E-Mail benachrichtigt werden möchten, müssen Sie die Einstellungen für das Senden der Benachrichtigungen vornehmen.

Gehen Sie folgendermaßen vor, um das Senden von E-Mail-Benachrichtigungen anzupassen:

1. Öffnen Sie das Programmkonfigurationsfenster.
2. Wählen Sie auf der linken Fensterseite ein Abschnitt **Einstellungen**.
3. Aktivieren Sie im Block **Ansicht** das Kontrollkästchen **Ereignisbenachrichtigung aktivieren** und klicken Sie auf die Schaltfläche **Einstellungen**.
4. Aktivieren Sie im folgenden Fenster .**Benachrichtigungseinstellungen** die Kontrollkästchen für die erforderlichen Ereignisse in der Spalte **E-Mail** und klicken Sie auf die Schaltfläche**E-Mail-Einstellungen**.
5. Geben Sie im folgenden Fenster **Anpassen von E-Mail-Benachrichtigungen** die erforderlichen Parameterwerte an. Erstellen Sie zur Benachrichtigung über Ereignisse nach einem bestimmten Zeitraum einen Zeitplan für das Senden von Nachrichten. Klicken Sie dazu auf die Schaltfläche **Ändern**. Nehmen Sie im folgenden Fenster **Zeitplan** die erforderlichen Änderungen vor.

PARAMETER DES EREIGNISBERICHTS

Kaspersky Anti-Virus bietet die Möglichkeit, Informationen über Ereignisse, die bei der Arbeit der Anwendung eintreten, im allgemeinen Ereignisbericht von Microsoft Windows (**Anwendung**) oder in einem separaten Ereignisbericht von Kaspersky Anti-Virus (**Kaspersky Event Log**) aufzuzeichnen.

Zur Ansicht von Berichten dient das Standardfenster von Microsoft Windows **Ereignisanzeige (Event Viewer)**, das mit folgendem Befehl geöffnet wird: **Start/Einstellungen/Systemsteuerung/Verwaltung/Ereignisanzeige**.

Gehen Sie folgendermaßen vor, um die Parameter des Ereignisberichts anzupassen:

1. Öffnen Sie das Programmkonfigurationsfenster.
2. Wählen Sie auf der linken Fensterseite ein Abschnitt **Einstellungen**.
3. Aktivieren Sie im Block **Ansicht** das Kontrollkästchen **Ereignisbenachrichtigung aktivieren** und klicken Sie auf die Schaltfläche **Einstellungen**.
4. Aktivieren Sie im folgenden Fenster .**Benachrichtigungseinstellungen** die Kontrollkästchen für die erforderlichen Ereignisse in der Spalte **Bericht** und klicken Sie auf die Schaltfläche **Berichtseinstellungen**.
5. Wählen Sie im folgenden Fenster **Einstellungen für Ereignisbericht** einen Bericht aus, in dem die Ereignisdaten gespeichert werden sollen.

AKTIVE ELEMENTE DER BENUTZEROBERFLÄCHE

Unter aktiven Elementen der Benutzeroberfläche werden folgende Optionen für Kaspersky Anti-Virus verstanden:

Animation des Symbols im Infobereich der Taskleiste.

In Abhängigkeit von der ausgeführten Programmaktion ändert sich das Symbol im Infobereich. Wird beispielsweise die Untersuchung eines Skripts ausgeführt, dann erscheint im Hintergrund des Symbols ein kleines Piktogramm mit einem Skript. Die Animation des Programmsymbols wird standardmäßig verwendet. Das Symbol gibt in diesem Fall nur den Schutzstatus Ihres Computers wieder: Wenn der Schutz aktiviert ist, ist das Symbol farbig. Wenn der Schutz angehalten oder ausgeschaltet wurde, nimmt das Symbol graue Farbe an.

"Protected by Kaspersky Lab" über dem Microsoft Windows-Begrüßungsbildschirm anzeigen.

Dieser Indikator erscheint in der Grundeinstellung rechts oben am Bildschirmrand, wenn Kaspersky Anti-Virus gestartet wird. Er informiert darüber, dass der Schutz Ihres Computers vor jeder Art von Bedrohung aktiviert ist.

Gehen Sie folgendermaßen vor, um die aktiven Elemente der Benutzeroberfläche anzupassen:

1. Öffnen Sie das Programmkonfigurationsfenster.
2. Wählen Sie auf der linken Fensterseite ein Abschnitt **Einstellungen**.
3. Aktivieren Sie im Block **Ansicht** die entsprechenden Kontrollkästchen.

BERICHTE UND SPEICHER

Dieser Abschnitt enthält Parameter, die die Arbeit mit der Datenverwaltung des Programms regulieren.

Die *Datenverwaltung* umfasst Objekte, die während der Arbeit von Kaspersky Anti-Virus in der Quarantäne und im Backup gespeichert wurden, sowie Berichtsdateien über die Arbeit der Komponenten des Programms.

In diesem Abschnitt können Sie:

- Parameter für das Erstellen und Speichern von Berichten anpassen.
- Einstellungen für Quarantäne und Backup anpassen.
- Inhalt des Speichers für Berichte, Quarantäne und Backup bereinigen.

Gehen Sie folgendermaßen vor, um den Inhalt der Speicher zu bereinigen:

1. Öffnen Sie das Programmkonfigurationsfenster.
2. Wählen Sie auf der linken Fensterseite den Abschnitt **Berichte und Speicher**.
3. Klicken Sie im folgenden Fenster auf die Schaltfläche **Leeren**.
4. Geben Sie im folgenden Fenster **Datenverwaltung** an, welche Speicher bereinigt werden sollen.

SIEHE AUCH

PRINZIPIEN DER ARBEIT MIT BERICHTEN

Die Arbeit von Datei-Anti-Virus und die Ausführung von Untersuchungs- und Updateaufgaben werden in einem Bericht protokolliert.

Gehen Sie folgendermaßen vor, um die Berichte anzuzeigen:

1. Öffnen Sie das Programmhauptfenster.
2. Klicken Sie auf die Schaltfläche **Berichte**.

Gehen Sie folgendermaßen vor, um sich über alle Ereignisse zu informieren, die im Bericht über eine Komponente oder über die Aufgabenausführung aufgezeichnet wurden:

1. Öffnen Sie das Programmhauptfenster und klicken Sie auf die Schaltfläche **Berichte**.
2. Wählen Sie im folgenden Fenster auf der Registerkarte **Berichte** den Namen einer Komponente oder Aufgabe aus und klicken Sie auf die Schaltfläche **Details**. Dadurch wird ein Fenster geöffnet, das Detailinformationen über die Arbeit von Datei-Anti-Virus oder der Aufgabe enthält. Die Ergebnisstatistik der Arbeit befindet sich im oberen Fensterbereich, ausführliche Informationen befinden sich auf verschiedenen Registerkarten im mittleren Bereich. Abhängig davon, ob der Bericht für Datei-Anti-Virus oder für eine Aufgabe ausgewählt wurde, kann sich der Aufbau der Registerkarten unterscheiden.

Gehen Sie folgendermaßen vor, um einen Bericht in eine Textdatei zu importieren:

1. Öffnen Sie das Programmhauptfenster und klicken Sie auf die Schaltfläche **Berichte**.
2. Wählen Sie im folgenden Fenster auf der Registerkarte **Berichte** den Namen einer Komponente oder Aufgabe aus und klicken Sie auf die Schaltfläche **Details**.
3. Das folgende Fenster enthält Informationen über die Arbeit der gewählten Komponente oder Aufgabe. Klicken Sie auf die Schaltfläche **Speichern als** und geben Sie an, wo die Berichtsdatei gespeichert werden soll.

ANPASSEN DER BERICHTSPARAMETER

Sie können folgende Parameter für das Erstellen und Speichern von Berichten anpassen:

- Erlauben oder Verbieten, dass Ereignisse mit rein informativem Charakter im Bericht aufgezeichnet werden. In der Regel sind solche Ereignisse nicht für den Schutz wichtig (Kontrollkästchen ☑ **Informative Ereignisse protokollieren**).
- Festlegen, dass nur Ereignisse gespeichert werden, die beim letzten Start der Aufgabe eingetreten sind. Dadurch kann Festplattenplatz gespart werden, weil der Bericht eine geringere Größe erhält (Kontrollkästchen ☑ **Nur aktuelle Ereignisse speichern**). Wenn das Kontrollkästchen aktiviert ist, werden die Informationen im Bericht bei jedem Neustart der Aufgabe aktualisiert. Allerdings werden nur Informationen mit rein informativem Charakter überschrieben.
- Bestimmen, wie lange Berichte gespeichert werden sollen (Kontrollkästchen ☑ **Berichte speichern für maximal**). Der Standardwert für die Speicherdauer von Berichten beträgt 30 Tage. Danach werden die Berichte gelöscht. Sie können die maximale Speicherdauer ändern oder diese Beschränkung völlig aufheben.
- Maximale Größe des Berichts festlegen (Kontrollkästchen ☑ **Maximale Größe**). Die maximale Größe beträgt standardmäßig 250 MB. Sie können die Größenbeschränkung aufheben oder einen anderen Wert festlegen.

Gehen Sie folgendermaßen vor, um die Parameter für das Anlegen und Speichern von Berichten anzupassen:

1. Öffnen Sie das Programmkonfigurationsfenster.
2. Wählen Sie auf der linken Fensterseite den Abschnitt **Berichte und Speicher**.
3. Aktivieren Sie im Block **Berichte** die entsprechenden Kontrollkästchen und legen Sie bei Bedarf die Speicherdauer für Berichte und eine maximale Berichtsgröße fest.

QUARANTÄNE FÜR MÖGLICHERWEISE INFIZIERTE OBJEKTE

Die **Quarantäne** ist ein spezieller Speicher, in den Objekte verschoben werden, die möglicherweise von Viren infiziert sind.

Möglicherweise infizierte Objekte sind Objekte, die verdächtig sind, von Viren oder Virenmodifikationen infiziert zu sein.

Warum *möglicherweise infiziert*? Es ist nicht immer möglich, eindeutig festzustellen, ob ein Objekt infiziert ist oder nicht. Dafür gibt es folgende Gründe:

- *Der Code des analysierten Objekts besitzt Ähnlichkeit mit einer bekannten Bedrohung, wurde aber teilweise verändert*.

  Die Programm-Datenbanken enthalten alle Bedrohungen, die bisher von den Kaspersky-Lab-Spezialisten untersucht wurden. Wenn ein Schadprogramm verändert wird und diese Veränderungen noch nicht in die Signaturen aufgenommen wurden, klassifiziert Kaspersky Anti-Virus das Objekt, das von einem veränderten Schadprogramm infiziert ist, als möglicherweise infiziertes Objekt und informiert darüber, welcher Bedrohung diese Infektion ähnelt.

- *Der Code des gefundenen Objekts erinnert an die Struktur eines Schadprogramms. Die Bedrohungssignaturen enthalten jedoch keine entsprechenden Einträge*.

  Es ist durchaus möglich, dass es sich um eine neue Art von Bedrohung handelt. Deshalb stuft Kaspersky Anti-Virus das Objekt als möglicherweise infiziert ein.

Der Verdacht, dass eine Datei durch einen Virus infiziert ist, wird mit dem *heuristischen Code Analysator* ermittelt, mit dessen Hilfe bis zu 92 % neuer Viren erkannt werden. Dieser Mechanismus ist sehr effektiv und führt nur selten zu Fehlalarmen.

Ein verdächtiges Objekt kann während der Virensuche sowie bei der Arbeit von Datei-Anti-Virus gefunden und in die Quarantäne verschoben werden.

Ein Objekt unter Quarantäne zu stellen, bedeutet, es wird nicht kopiert, sondern verschoben: Das Objekt wird am ursprünglichen Speicherort oder aus einer E-Mail-Nachricht gelöscht und im Quarantäneordner gespeichert. Die unter Quarantäne stehenden Dateien werden in einem speziellen Format gespeichert und stellen keine Gefahr dar.

SIEHE AUCH

Arbeit mit Objekten in der Quarantäne 92

ARBEIT MIT OBJEKTEN IN DER QUARANTÄNE

Mit Objekten, die in die Quarantäne verschoben wurden, können Sie folgende Aktionen ausführen:

- Dateien, die Sie für infiziert halten, in die Quarantäne verschieben.
- Alle möglicherweise infizierten Quarantäneobjekte unter Verwendung der aktuellen Version der Programm-Datenbanken untersuchen und desinfizieren.
- Dateien wiederherstellen entweder in einem vom Benutzer gewählten Ordner oder in den Ordnern, aus denen sie (standardmäßig) in die Quarantäne verschoben wurden.
- Ein beliebiges Quarantäneobjekt oder eine Gruppe ausgewählter Objekte löschen.

➧ *Gehen Sie folgendermaßen vor, um mit Quarantäneobjekten zu arbeiten:*

1. Öffnen Sie das Programmhauptfenster und klicken Sie auf die Schaltfläche **Gefunden**.

2. Führen Sie im folgenden Fenster auf der Registerkarte **Quarantäne** die entsprechenden Aktionen aus.

SICHERUNGSKOPIEN GEFÄHRLICHER OBJEKTE

Bei der Desinfektion von Objekten kann es vorkommen, dass es nicht gelingt, die Objekte vollständig zu erhalten. Wenn ein desinfiziertes Objekt wichtige Informationen enthielt, die aufgrund der Desinfektion vollständig oder teilweise verloren gingen, kann versucht werden, das ursprüngliche Objekt über seine Sicherungskopie wiederherzustellen.

Eine **Sicherungskopie** ist eine Kopie des gefährlichen Originalobjekts. Sie wird bei der ersten Desinfektion oder beim Löschen des Objekts erstellt und im Backup gespeichert.

Das **Backup** ist ein spezieller Speicher für Sicherungskopien gefährlicher Objekte, die verarbeitet oder gelöscht werden. Die Hauptfunktion des Backups besteht in der Möglichkeit, das ursprüngliche Objekt jederzeit wiederherzustellen. Die Sicherungskopien werden im Backup in einem speziellen Format gespeichert und stellen keine Gefahr dar.

SIEHE AUCH

Arbeit mit Sicherungskopien 93

ARBEIT MIT SICHERUNGSKOPIEN

Mit Objekten, die im Backup gespeichert wurden, können Sie folgende Aktionen ausführen:

- bestimmte Kopien wiederherstellen.
- Objekte löschen.

Gehen Sie folgendermaßen vor, um mit Backup-Objekten zu arbeiten:

1. Öffnen Sie das Programmhauptfenster und klicken Sie auf die Schaltfläche **Gefunden**.
2. Führen Sie im folgenden Fenster auf der Registerkarte **Backup** die entsprechenden Aktionen aus.

EINSTELLUNGEN FÜR QUARANTÄNE UND BACKUP ANPASSEN

Sie können folgende Parameter für Quarantäne und Backup anpassen:

- Sie können festlegen, dass die Quarantäneobjekte jedes Mal nach der Aktualisierung der Programm-Datenbanken untersucht werden sollen (Kontrollkästchen ☑ **Quarantänedateien nach jedem Update untersuchen**).

  Kaspersky Anti-Virus kann die Quarantäneobjekte nicht sofort nach dem Datenbank-Update untersucht, wenn Sie gerade mit der Quarantäne arbeiten.

- Legen Sie eine maximale Speicherdauer für Objekte in der Quarantäne und Sicherungskopien im Backup fest (Kontrollkästchen ☑ **Objekte speichern für maximal**). Standardmäßig beträgt die Speicherdauer für Quarantäneobjekte 90 Tage. Danach werden die Objekte gelöscht. Sie können die maximale Speicherdauer ändern oder diese Beschränkung völlig aufheben.

- Eine maximale Größe für den Datenspeicher festlegen (Kontrollkästchen ☑ **Maximale Größe**). Die maximale Größe beträgt standardmäßig 1000 MB. Sie können die Größenbeschränkung aufheben oder einen anderen Wert festlegen.

➡ Gehen Sie folgendermaßen vor, um die Parameter für die Quarantäne und das Backup anzupassen:

1. Öffnen Sie das Programmkonfigurationsfenster.
2. Wählen Sie auf der linken Fensterseite den Abschnitt **Berichte und Speicher**.
3. Aktivieren Sie im Block **Quarantäne und Backup** die entsprechenden Kontrollkästchen und legen Sie bei Bedarf eine maximale Größe für den Datenspeicher fest.

NOTFALL-CD

Kaspersky Anti-Virus enthält einen Dienst zum Erstellen einer Rettungs-Disk.

Die Rettungs-Disk dient zur Untersuchung und Desinfektion infizierter x86-kompatibler Computer. Sie kommt dann zum Einsatz, wenn der Infektionsgrad so hoch ist, dass die Desinfektion eines Computers nicht mehr mit Hilfe von Antiviren-Anwendungen oder Desinfektionstools (z.B. Kaspersky AVPTool) möglich ist, die unter dem Betriebssystem gestartet werden. Dabei wird die Effektivität der Desinfektion gesteigert, weil die im System vorhandenen Schädlinge nicht die Kontrolle übernehmen können, während das Betriebssystem hochgefahren wird.

Eine Rettungs-Disk wird auf Basis eines Linux-Betriebssystemkerns erstellt und ist eine iso-Datei, die folgende Elemente umfasst:

- System- und Konfigurationsdateien für Linux.
- Eine Auswahl von Tools zur Betriebssystemdiagnose.
- Auswahl von sonstigen Utilities (Datei-Manager u.a.).
- Dateien für Kaspersky Rescue Disk.
- Dateien, die die Programm-Datenbanken enthalten.

Ein Computer, dessen Betriebssystem beschädigt ist, kann auf zwei Arten hochgefahren werden:

- *lokal*, aus dem CD/DVD-ROM-Laufwerk. Dafür muss auf dem Computer ein entsprechendes Gerät installiert sein.
- *im Remote-Modus*, vom Arbeitsplatz des Administrators oder von einem anderen Netzwerkcomputer aus.

Das Booten im Remote-Modus ist nur dann möglich, wenn der hochzufahrende Computer die Technologie Intel® vPro™ oder Intel® Active Management unterstützt.

➡ *Gehen Sie folgendermaßen vor, um eine Rettungs-Disk zu erstellen:*

1. Öffnen Sie das Programmhauptfenster.
2. Klicken Sie auf die Schaltfläche **Notfall-CD**, um den Assistenten für die Notfall-CD (s. S. 95) zu starten.
3. Folgen Sie den Anweisungen des Assistenten.
4. Verwenden Sie die Datei, die mit Hilfe des Assistenten erstellt wurde, um eine Bootdisk (CD/DVD) zu brennen. Dafür kann ein Brennprogramm für CDs / DVDs (z.B. Nero) eingesetzt werden.

SIEHE AUCH

ERSTELLEN EINER NOTFALL-CD ZUR SYSTEMWIEDERHERSTELLUNG

Das Anlegen einer Rettungs-Disk umfasst das Erstellen eines Disk-Image (iso-Datei) mit den aktuellen Programm-Datenbanken und Konfigurationsdateien.

Ein Original des Disk-Image, auf dessen Basis eine neue Datei erstellt wird, kann von einem Kaspersky-Lab-Server heruntergeladen oder aus einer lokalen Quelle kopiert werden.

Die Abbild-Datei, die vom Assistenten erstellt wurde, wird unter dem Namen *rescuecd.iso* im Ordner "*Documents and Settings\All Users\Application Data\Kaspersky Lab\AVP80\Data\Rdisk*" ("*ProgramData\Kaspersky Lab\AVP80\Data\Rdisk*" – für Microsoft Vista) abgelegt. Wenn der Assistent im angegebenen Ordner eine früher erstellte Image-Datei gefunden hat, aktivieren Sie das Kontrollkästchen ☑ **Vorhandenes Image verwenden**. Sie können die Datei als Basis für das Disk-Image verwenden und sofort mit Schritt 3 - Image aktualisieren (s. S. 96) fortfahren. Wenn der Assistent keine Abbild-Datei gefunden hat, fehlt dieses Kontrollkästchen.

Die Rettungs-Disk wird mit Hilfe eines Assistenten erstellt, der aus einer Reihe von Fenstern (Schritten) besteht. Zur Navigation zwischen den Fenstern dienen die Schaltflächen **Zurück** und **Weiter**, zum Abschluss des Assistenten die Schaltfläche **Fertig**. Die Arbeit des Assistenten kann auf einer beliebigen Etappe durch Klick auf die Schaltfläche **Abbrechen** beendet werden.

AUSFÜHRLICHE BESCHREIBUNG DER SCHRITTE DES ASSISTENTEN

SCHRITT 1. QUELLE FÜR DISK-IMAGE WÄHLEN

Wenn Sie im vorherigen Fenster des Assistenten das Kontrollkästchen ☑ **Vorhandenes Abbild verwenden**, aktiviert haben, wird dieser Schritt übersprungen.

Auf dieser Etappe muss aus folgenden Varianten eine Quelle für die Image-Datei gewählt werden:

- Wählen Sie die Variante ◉ **Image von CD/DVD oder aus lokalem Netzwerk kopieren**, wenn Sie über eine fertige Rettungs-Disk (CD/DVD) verfügen oder auf Ihrem Computer bzw. in einer Ressource des lokalen Netzwerks ein dafür vorbereitetes Image bereitliegt.

- Wählen Sie die Variante ◉ **Image von Kaspersky-Lab-Server herunterladen**, wenn Sie nicht über eine fertige Image-Datei verfügen. Sie können diese von einem Kaspersky-Lab-Server herunterladen (Die Dateigröße beträgt ungefähr 100 MB).

SCHRITT 2. DISK-ABBILD KOPIEREN (HERUNTERLADEN)

Wenn Sie beim vorherigen Schritt die Variante zum Kopieren des Image aus einer lokalen Quelle gewählt haben (**Image von CD/DVD oder aus lokalem Netzwerk kopieren**), geben Sie bei diesem Schritt den entsprechenden Pfad an. Verwenden Sie dazu die Schaltfläche **Durchsuchen**. Anschließend wird angezeigt, wie das Kopieren der Datei verläuft.

Wenn Sie die Variante **Image von Kaspersky-Lab-Server herunterladen**, gewählt haben, wird sofort angezeigt, wie das Kopieren der Datei verläuft.

SCHRITT 3. ABBILD-DATEI AKTUALISIEREN

Der Vorgang zur Aktualisierung der Image-Datei umfasst:

- Aktualisierung der Programm-Datenbanken.
- Aktualisierung der Konfigurationsdateien.

Die Konfigurationsdateien legen fest, ob die Rettungs-Disk auf einem lokalen oder auf einem Remote-Computer verwendet wird. Deshalb muss vor der Aktualisierung der Image-Datei eine der folgenden Varianten gewählt werden:

- **Remote-Computer hochfahren**, wenn geplant ist, den Remote-Computer zu booten.

  Beachten Sie, dass der Remote-Computer die Technologie Intel® vPro™ oder Intel® Active Management unterstützen muss, um auf diese Weise hochgefahren werden zu können.

  Wenn die Internetverbindung des Remote-Computers über einen Proxyserver erfolgt, steht bei der Verwendung der Rettungs-Disk das Update nicht zur Verfügung. In diesem Fall wird empfohlen, Kaspersky Anti-Virus vorher zu aktualisieren.

- **System von CD/DVD hochfahren**, wenn das zu erstellende Disk-Image später auf CD/DVD gebrannt werden soll.

Wählen Sie eine Variante aus und klicken Sie dann auf die Schaltfläche **Weiter**. Im nächsten Fenster des Assistenten wird angezeigt, wie die Aktualisierung verläuft.

Wenn die Variante **Remote-Computer hochfahren** gewählt wurde, kann das erstellte Image nicht verwendet werden, um eine CD/DVD zu brennen und anschließend einen Computer hochzufahren. Um einen Computer von CD/DVD zu booten, muss der Assistent erneut gestartet und bei diesem Schritt die Variante **System von CD/DVD hochfahren** gewählt werden.

SCHRITT 4. REMOTE-COMPUTER HOCHFAHREN

Dieser Schritt des Assistenten erfolgt, wenn Sie beim vorherigen Schritt die Variante **Remote-Computer hochfahren** gewählt haben.

Geben Sie die Daten des Computers an:

- **IP-Adresse oder Computername** im Netzwerk.
- Daten eines Benutzerkontos mit Administratorrechten: **Benutzername** und **Kennwort**.

Das folgende Fenster des Assistenten ist eine iAMT-Konsole, in der Sie den Prozess zum Hochfahren des Computers (s. S. 97) steuern können.

SCHRITT 5. ASSISTENT ABSCHLIEßEN

In diesem Fenster informiert der Assistent Sie darüber, dass die Rettungs-Disk erfolgreich erstellt wurde.

HOCHFAHREN EINES COMPUTERS MIT HILFE DER NOTFALL-CD

Wenn sich das Betriebssystem aufgrund eines Virenangriffs nicht mehr hochfahren lässt, können Sie die Notfall-CD einsetzen.

Um das Betriebssystem hochzufahren, ist eine Image-Datei (.iso) der Boot-Disk erforderlich. Sie können die Datei von einem Kaspersky-Lab-Server herunterladen (s. S. 95) oder eine vorhandene Datei aktualisieren (s. S. 96).

Im Folgenden wird die Arbeit der Rettungs-Disk ausführlich erläutert. Während des Downloads der Datei finden folgende Operationen statt:

1. Die Hardware des Computers wird automatisch ermittelt.

2. Auf den Festplatten wird nach Dateisystemen gesucht. Gefundene Dateisysteme erhalten einen Namen, der mit *C* beginnt.

   Die Namen, die den Festplatten und Wechselmedien zugewiesen werden, können von ihren Namen im Betriebssystem abweichen.

   Wenn sich das Betriebssystem des Computers, der hochgefahren werden soll, im Ruhezustand befindet oder das Dateisystem den Status *unclean* besitzt, weil beim Herunterfahren ein Fehler aufgetreten ist, können Sie entscheiden, ob das Dateisystem gemountet oder der Computer neu gestartet werden soll.

   Das Mounten des Dateisystems kann zu seiner Beschädigung führen.

3. Die Auslagerungsdatei von Microsoft Windows *pagefile.sys* wird gesucht. Wenn sie nicht vorhanden ist, wird die Größe des virtuellen Speichers durch die Größe des Arbeitsspeichers begrenzt.

4. Eine Sprache wird ausgewählt. Wenn innerhalb einer bestimmten Zeit keine Auswahl stattfindet, wird standardmäßig die Sprache Englisch gewählt.

   Beim Hochfahren eines Remote-Computers fehlt dieser Schritt.

5. Es werden Ordner zum Speichern von Antiviren-Datenbanken, Berichten, Quarantäne und sonstigen Dateien gesucht (erstellt). In der Grundeinstellung werden die Ordner des Kaspersky-Lab-Programms verwendet, das auf dem infizierten Computer installiert ist (*ProgramData/Kaspersky Lab/AVP8* – für Microsoft Windows Vista, *Documents and Settings/All Users/Application Data/Kaspersky Lab/AVP8* – für ältere Versionen von Microsoft Windows). Wenn diese Ordner des Programms nicht gefunden werden, wird versucht, sie zu erstellen. Falls die Ordner nicht gefunden wurden und nicht erstellt werden können, wird auf einem der Laufwerke der Ordner *kl.files* erstellt.

6. Es wird versucht, mit Hilfe der Daten, die in den Systemdateien des hochzufahrenden Computers gefunden werden, die Netzwerkverbindungen anzupassen.

7. Das grafische Subsystem wird geladen und Kaspersky Rescue Disk wird gestartet (beim Booten des Computers von CD/DVD).

   Beim Hochfahren eines Remote-Computers wird die Befehlszeile in die iAMT-Konsole geladen. Zur Verwaltung von Aufgaben dienen die Befehle für die Arbeit mit Kaspersky Rescue Disk aus der Befehlszeile (s. S. 99).

Im Rettungsmodus sind nur die Aufgaben zur Virensuche und zum Update der Datenbanken aus einer lokalen Quelle verfügbar, sowie das Rollback für Updates und die Anzeige der Statistik.

- *Gehen Sie folgendermaßen vor, um das Betriebssystem des infizierten Computers von CD/DVD-ROM zu booten:*

  1. Wählen Sie in den BIOS-Einstellungen das Booten von CD/DVD-ROM (weitere Informationen können der Dokumentation zum Motherboard Ihres Computers entnommen werden).

  2. Legen Sie die Disk, auf die das Disk-Image gebrannt wurde, in das CD/DVD-Laufwerk des infizierten Computers ein.

  3. Starten Sie den Computer neu.

  4. Danach wird der Computer nach dem oben beschriebenen Algorithmus hochgefahren.

- *Gehen Sie folgendermaßen vor, um das Betriebssystem des Remote-Computers hochzufahren:*

  1. Öffnen Sie das Programmhauptfenster.

  2. Klicken Sie auf die Schaltfläche Notfall-CD (s. S. 95), um den **Assistenten für die Notfall-CD** zu starten. Folgen Sie den Anweisungen des Assistenten.

     Beachten Sie, dass auf der Etappe zur Aktualisierung (s. S. 96) des Disk-Image die Variante **Remote-Computer hochfahren gewählt werden muss**.

Danach wird der Computer nach dem oben beschriebenen Algorithmus hochgefahren.

ARBEIT MIT KASPERSKY RESCUE DISK AUS DER BEFEHLSZEILE

Sie können Kaspersky Rescue Disk mit Hilfe der Befehlszeile steuern. Dabei ist die Möglichkeit zum Ausführen der folgenden Operationen vorgesehen:

- Untersuchung von ausgewählten Objekten.
- Update der Datenbanken und Module des Programms.
- Rollback zum vorherigen Update
- Aufruf der Hilfe über die Syntax der Befehlszeile.
- Aufruf der Hilfe über die Syntax eines Befehls.

Syntax der Befehlszeile:

```
<Befehl> [Parameter]
```

Als <Befehl> werden verwendet:

HELP	Hilfe über die Befehlssyntax, Anzeige einer Befehlsliste
SCAN	Untersuchung von Objekten auf das Vorhandensein von Viren
UPDATE	Updateaufgabe starten
ROLLBACK	Rollback zum vorherigen Update
EXIT	Arbeit von Kaspersky Rescue Disk beenden

IN DIESEM ABSCHNITT

VIRENSUCHE

Die Befehlszeile zum Starten der Virenuntersuchung eines bestimmten Bereichs und zur Verarbeitung von schädlichen Objekten besitzt generell folgendes Aussehen:

```
SCAN [<Untersuchungsobjekt>] [<Aktion>] [<Dateitypen>] [<Ausnahmen>]
[<Berichtsparameter>]
```

Beschreibung der Parameter:

<Untersuchungsobjekt> – Der Parameter gibt eine Liste der Objekte an, die auf das Vorhandensein von schädlichem Code untersucht werden sollen. Der Parameter kann mehrere Werte aus der folgenden Liste enthalten. Die Werte werden durch Leerzeichen getrennt.	
<files>	Liste mit den Pfaden der Dateien und / oder Ordner für die Untersuchung. Die Angabe des absoluten oder relativen Pfads der Datei ist zulässig. Als Trennzeichen für die Elemente der Liste dient das Leerzeichen. Kommentare: • Wenn der Objektname ein Leerzeichen enthält, wird er in Anführungszeichen gesetzt. • Wenn ein konkreter Ordner angegeben wird, werden alle darin enthaltenen Dateien untersucht.
/discs/	Alle Laufwerke untersuchen
/discs/<disc_name>:/<folder>	Einen bestimmten Ordner untersuchen, wobei <disc_name> – Name des Laufwerks, und <folder> – Pfad des zu untersuchenden Ordners.
<Aktion> – Der Parameter bestimmt die Aktionen mit einem schädlichen Objekt, das während der Untersuchung gefunden wird. Wenn der Parameter nicht angegeben wird, wird standardmäßig die Aktion ausgeführt, die dem Wert **i8** entspricht.	
-i0	Keine Aktion ausführen, nur Informationen im Bericht protokollieren.
-i1	infizierte Objekte desinfizieren; wenn die Desinfektion nicht möglich ist – überspringen**.**
-i2	Infizierte Objekte desinfizieren; wenn die Desinfektion nicht möglich ist – löschen; infizierte Objekte aus Containern (zusammengesetzten Objekten) nicht löschen; Container mit ausführbarer Kopfzeile (sfx-Archive) löschen.
-i3	infizierte Objekte desinfizieren; wenn die Desinfektion nicht möglich ist – löschen; Container-Objekte vollständig löschen, wenn die darin enthaltenen infizierten Dateien nicht gelöscht werden können.
-i4	infizierte Objekte löschen; Container-Objekte vollständig löschen, wenn die darin enthaltenen infizierten Dateien nicht gelöscht werden können.
-i8	Beim Fund eines infizierten Objekts den Benutzer nach der Aktion fragen.
-i9	Den Benutzer nach der Aktion fragen, wenn die Untersuchung abgeschlossen wird.
<Dateitypen> – Der Parameter bestimmt die Typen der Dateien, die der Virenuntersuchung unterzogen werden. Wenn der Parameter nicht angegeben wird, werden standardmäßig nur infizierbare Dateien nach ihrem Inhalt untersucht.	

-fe	Nur infizierbare Dateien nach Erweiterung untersuchen.
-fi	Nur infizierbare Dateien nach Inhalt untersuchen.
-fa	**Alle Dateien untersuchen**.
<Ausnahmen> – Der Parameter bestimmt die Objekte, die von der Untersuchung ausgeschlossen werden sollen. Der Parameter kann mehrere Werte aus der folgenden Liste enthalten. Die Werte werden durch Leerzeichen getrennt.	
-e:a	Archive nicht untersuchen.
-e:b	Mail-Datenbanken nicht untersuchen.
-e:m	E-Mail-Nachrichten im Format plain text nicht untersuchen.
-e:<filemask>	Objekte nach Maske nicht untersuchen.
-e:<Sekunden>	Objekte überspringen, deren Untersuchung länger dauert, als der durch den Parameter **<seconds>** angegebene Zeitraum.
-es:<Größe>	Objekte überspringen, deren Größe (in MB) über dem Wert liegt, der durch den Parameter **<size>** angegeben wird.

Beispiele:

- *Untersuchung des Verzeichnisses Documents and Settings und des Laufwerks <D> starten:*

```
SCAN /discs/D: "/discs/C:/Documents and Settings"
```

UPDATE VON KASPERSKY ANTI-VIRUS

Der Befehl für das Update der Programm-Module und Bedrohungssignaturen von Kaspersky Anti-Virus besitzt folgende Syntax:

```
UPDATE [<Updatequelle>] [-R[A]:<Berichtsdatei>]
```

Beschreibung der Parameter:

<Updatequelle>	HTTP-, FTP-Server oder Netzwerkordner für den Download von Updates. Als Wert für diesen Parameter kann der vollständige Pfad oder die URL-Adresse der Updatequelle angegeben werden. Wenn der Pfad nicht angegeben wird, wird die Updatequelle aus den Parametern des Diensts für das Update von Kaspersky Anti-Virus übernommen.
-R[A]:<Berichtsdatei>	**-R:<Berichtsdatei> –** nur wichtige Ereignisse im Bericht protokollieren. **-RA:<Berichtsdatei> –** alle Ereignisse im Bericht protokollieren. Die Angabe des absoluten Pfads der Datei ist zulässig. Wenn der Parameter nicht angegeben wird, werden die Untersuchungsergebnisse auf dem Bildschirm angezeigt, alle Ereignisse werden angezeigt.

Beispiele:

- *Update der Datenbanken, alle Ereignisse im Bericht protokollieren:*

```
UPDATE -RA:/discs/C:/avbases_upd.txt
```

ROLLBACK ZUM VORHERIGEN UPDATE

Befehlssyntax:

```
ROLLBACK [-R[A]:<Berichtsdatei>]
```

Beschreibung der Parameter:

-R[A]:<Berichtsdatei>	**-R:<Berichtsdatei> –** nur wichtige Ereignisse im Bericht protokollieren. **-RA:<Berichtsdatei> –** alle Ereignisse im Bericht protokollieren. Die Angabe des absoluten Pfads der Datei ist zulässig. Wenn der Parameter nicht angegeben wird, werden die Untersuchungsergebnisse auf dem Bildschirm angezeigt, alle Ereignisse werden angezeigt.

Beispiel:

```
ROLLBACK -RA:/discs/C:/avbases_upd.txt
```

ANZEIGEN DER HILFE

Zur Anzeige der Hilfe über die Syntax der Befehlzeile dient folgender Befehl:

```
[ -? | HELP ]
```

Um Hilfe über die Syntax eines konkreten Befehls zu erhalten, können Sie einen der folgenden Befehle verwenden:

```
<Befehl> -?
HELP <Befehl>
```

ÜBERPRÜFUNG DER EINSTELLUNGEN VON KASPERSKY ANTI-VIRUS

Nach der Installation und Konfiguration von Kaspersky Anti-Virus können Sie mit Hilfe eines "Testvirus" und dessen Modifikationen prüfen, ob die Einstellungen korrekt sind. Die Prüfung muss für jede Schutzkomponente und für jedes Protokoll einzeln ausgeführt werden.

In diesem Abschnitt

EICAR-"Testvirus" und seine Modifikationen

Dieser "Testvirus" wurde vom Institut eicar (The European Institute for Computer Antivirus Research) speziell zum Überprüfen der Arbeit von Antiviren-Produkten entwickelt.

Der "Testvirus" IST KEIN VIRUS und enthält keinen Programmcode, der Ihren Rechner beschädigen könnte. Trotzdem wird er von den meisten Antiviren-Softwareprodukten als Virus identifiziert.

Verwenden Sie nie echte Viren, um die Funktionsfähigkeit eines Antiviren-Produkts zu testen!

Der "Testvirus" kann von der offiziellen Internetseite des **EICAR**-Instituts heruntergeladen werden: http://www.eicar.org/anti_virus_test_file.htm.

Bevor der "Testvirus" heruntergeladen wird, muss der Antiviren-Schutz deaktiviert werden, weil die Datei *anti_virus_test_file.htm* andernfalls als infiziertes, mit dem HTTP-Protokoll übertragenes Objekt identifiziert und entsprechend behandelt wird. Vergessen Sie nicht, den Antiviren-Schutz sofort nach dem Download des "Testvirus" wieder zu aktivieren.

Die von der Webseite des **EICAR**-Instituts heruntergeladene Datei wird vom Programm als infiziertes Objekt identifiziert, das einen Virus enthält, **der nicht desinfiziert werden kann**, und führt die für diesen Objekttyp festgelegte Aktion aus.

Um die Funktion des Programms zu prüfen, können Sie auch Modifikationen des standardmäßigen "Testvirus" verwenden. Dazu wird der Inhalt des standardmäßigen "Testvirus" durch das Hinzufügen eines bestimmten Präfixes geändert (siehe Tabelle unten). Zum Erstellen von Modifikationen des "Testvirus" eignet sich ein beliebiger Text-Editor oder Hypertext-Editor wie beispielsweise **Microsoft Editor**, **UltraEdit32**, usw.

Die Prüfung der korrekten Funktion des Antiviren-Programms mit Hilfe eines modifizierten EICAR-"Testvirus" ist nur dann möglich, wenn die installierten Antiviren-Datenbanken nicht vor dem 24.10.2003 erschienen sind (kumulatives Update - Oktober 2003).

Die erste Spalte der Tabelle enthält Präfixe, die dem standardmäßigen "Testvirus" am Zeilenanfang hinzugefügt werden können. Die zweite Spalte zeigt die möglichen Werte für den Status, der einem Objekt aufgrund der Untersuchungsergebnisse von Anti-Virus zugewiesen werden kann. Die dritte Spalte bietet Informationen darüber, wie Objekte mit dem betreffenden Status vom Programm bearbeitet werden. Beachten Sie, dass die Aktionen für Objekte durch die Werte der Programmparameter bestimmt werden.

Nachdem dem "Testvirus" ein Präfix hinzugefügt wurde, speichern Sie die Datei z.B. unter dem Namen *eicar_dele.com*. Verwenden Sie die in der Tabelle angegebenen Namen für die modifizierten "Viren".

Tabelle 1. Modifikationen des "Testvirus"

Präfix	Status des Objekts	Informationen zur Verarbeitung des Objekts
Kein Präfix, standardmäßiger "Testvirus".	**Infiziert**. Das Objekt enthält einen bekannten Viruscode. Die Desinfektion ist nicht möglich.	Das Programm identifiziert dieses Objekt als Virus, der nicht desinfiziert werden kann. Beim Desinfektionsversuch des Objekts tritt ein Fehler auf und die für irreparable Objekte geltende Aktion wird ausgeführt.
CORR–	**Beschädigt.**	Das Programm hat Zugriff auf das Objekt erhalten, kann es aber aufgrund einer Beschädigung nicht untersuchen (z.B. beschädigte Struktur des Objekts, ungültiges Dateiformat). Informationen darüber, dass das Objekt verarbeitet wurde, können Sie dem Bericht über die Arbeit der Anwendung entnehmen.
WARN–	**Verdächtig**. Das Objekt enthält einen unbekannten Viruscode. Die Desinfektion ist nicht möglich.	Das Objekt wurde bei der heuristischen Analyse als verdächtig erkannt. Im Augenblick des Funds enthalten die Antiviren-Datenbanken keine Beschreibung zur Desinfektion dieses Objekts. Beim Fund eines solchen Objekts, erhalten Sie eine Meldung.
SUSP–	**Verdächtig**. Das Objekt enthält den modifizierten Code eines bekannten Virus. Die Desinfektion ist nicht möglich.	Das Programm hat erkannt, dass der Objektcode teilweise mit dem Code eines bekannten Virus übereinstimmt. Im Augenblick des Funds enthalten die Antiviren-Datenbanken keine Beschreibung zur Desinfektion dieses Objekts. Beim Fund eines solchen Objekts, erhalten Sie eine Meldung.
ERRO–	**Untersuchungsfehler**.	Bei der Untersuchung des Objekts ist ein Fehler aufgetreten. Die Anwendung erhielt keinen Zugriff auf das Objekt: Die Integrität des Objekts ist beschädigt (z.B. kein Endpunkt in einem Multi-Level-Archiv) oder die Verbindung zu dem Objekt fehlt (wenn ein Objekt in einer Netzwerkressource untersucht wird). Informationen darüber, dass das Objekt verarbeitet wurde, können Sie dem Bericht über die Arbeit der Anwendung entnehmen.
CURE–	**Infiziert**. Das Objekt enthält einen bekannten Viruscode. Die Desinfektion ist möglich.	Das Objekt enthält einen Virus, der desinfiziert werden kann. Das Programm führt die Desinfektion des Objekts aus, wobei der Text des Viruskörpers in CURE geändert wird. Beim Fund eines solchen Objekts, erhalten Sie eine Meldung.
DELE–	**Infiziert**. Das Objekt enthält einen bekannten Viruscode. Die Desinfektion ist nicht möglich.	Das Programm identifiziert dieses Objekt als Virus, der nicht desinfiziert werden kann. Beim Desinfektionsversuch des Objekts tritt ein Fehler auf und die für irreparable Objekte geltende Aktion wird ausgeführt. Beim Fund eines solchen Objekts, erhalten Sie eine Meldung.

ÜBERPRÜFUNG DER EINSTELLUNGEN VON DATEI-ANTI-VIRUS

➧ *Gehen Sie folgendermaßen vor, um zu prüfen, ob Datei-Anti-Virus korrekt eingestellt wurde:*

1. Erstellen Sie einen Ordner auf der Festplatte. Kopieren Sie den von der offiziellen Seite des **EICAR**-Instituts (http://www.eicar.org/anti_virus_test_file.htm) heruntergeladenen "Testvirus" und die von Ihnen erstellten Modifikationen des "Testvirus" in diesen Ordner.

2. Erlauben Sie das Protokollieren aller Ereignisse, damit Daten über beschädigte Objekte oder Objekte, die aufgrund einer Störung nicht untersucht werden, in der Berichtsdatei gespeichert werden.

3. Starten Sie den "Testvirus" oder seine Modifikation zur Ausführung.

Datei-Anti-Virus fängt den Zugriff auf die Datei ab, untersucht sie und führt die in den Einstellungen festgelegte Aktion aus. Durch die Auswahl unterschiedlicher Aktionsvarianten für ein gefundenes Objekt können Sie die Funktion der Komponente vollständig testen.

Vollständige Informationen über die Arbeitsergebnisse von Datei-Anti-Virus sind im Bericht über die Arbeit der Komponente enthalten.

ÜBERPRÜFUNG DER EINSTELLUNGEN FÜR EINE AUFGABE ZUR VIRENSUCHE

Gehen Sie folgendermaßen vor, um zu prüfen, ob eine Aufgabe zur Virensuche korrekt eingestellt wurde:

1. Erstellen Sie einen Ordner auf der Festplatte. Kopieren Sie den von der offiziellen Seite des **EICAR-Instituts** (http://www.eicar.org/anti_virus_test_file.htm) heruntergeladenen "Testvirus" und die von Ihnen erstellten Modifikationen des "Testvirus" in diesen Ordner.

2. Erstellen Sie eine neue Untersuchungsaufgabe und wählen Sie als Untersuchungsobjekt den Ordner, der die "Testviren" enthält.

3. Erlauben Sie das Protokollieren aller Ereignisse, damit Daten über beschädigte Objekte oder Objekte, die aufgrund einer Störung nicht untersucht werden, in der Berichtsdatei gespeichert werden.

4. Starten Sie die Ausführung der Untersuchungsaufgabe.

Wenn bei der Untersuchung verdächtige oder infizierte Objekte gefunden werden, werden die in den Einstellungen der Aufgabe festgelegten Aktionen ausgeführt. Durch die Auswahl unterschiedlicher Aktionsvarianten für ein gefundenes Objekt können Sie die Funktion der Komponente vollständig testen.

Vollständige Informationen über das Ausführungsergebnis der Untersuchungsaufgabe sind im Bericht über die Arbeit der Komponente enthalten.

ARTEN VON MELDUNGEN

Beim Eintreten bestimmter Ereignisse während der Arbeit von Kaspersky Anti-Virus werden auf dem Bildschirm spezielle Meldungen angezeigt. In Abhängigkeit davon, welche Relevanz das Ereignis für die Computersicherheit besitzt, sind folgende Arten von Meldungen möglich:

- **Alarm**. Ein Ereignis mit kritischer Priorität ist eingetreten. Beispiele: "Ein schädliches Objekt wurde gefunden" oder "Im System wurde eine gefährliche Aktivität erkannt". Die sofortige Entscheidung über das weitere Vorgehen ist erforderlich. Dieser Meldungstyp besitzt die Farbe Rot.

- **Warnung**. Ein potentiell gefährliches Ereignis hat sich ereignet. Beispiele: "Ein möglicherweise infiziertes Objekt wurde gefunden" oder "Im System wurde verdächtige Aktivität erkannt". Es muss entschieden werden, inwieweit das Ereignis nach Ihrem Ermessen gefährlich ist. Dieser Meldungstyp besitzt die Farbe Gelb.

- **Informationen**. Diese Meldung informiert über ein Ereignis, das keine vorrangige Priorität besitzt. Dieser Meldungstyp besitzt die Farbe Hellblau.

IN DIESEM ABSCHNITT

VERDÄCHTIGES OBJEKT WURDE GEFUNDEN

Wenn von Datei-Anti-Virus oder bei einer Untersuchungsaufgabe ein schädliches Objekt gefunden wird, erscheint eine spezielle Meldung auf dem Bildschirm.

Die Meldung enthält:

- Art der Bedrohung (beispielsweise *Virus*, *trojanisches Programm*) und Name des schädlichen Objekts, der seiner Bezeichnung in der Viren-Enzyklopädie von Kaspersky Lab entspricht. Der Name des schädlichen Objekts besitzt die Form eines Links zu der Ressource www.viruslist.de, die ausführliche Informationen darüber enthält, welche Art von Bedrohung auf dem Server gefunden wurde.

- Vollständiger Name und Pfad des schädlichen Objekts.

Ihnen wird angeboten, eine der folgenden Aktionen für das Objekt auszuwählen:

- **Desinfizieren** - Es wird versucht, das schädliche Objekt zu desinfizieren. Vor der Desinfektion wird eine Sicherungskopie des Objekts angelegt, um bei Bedarf das Objekt oder ein Infektionsbild wiederherstellen zu können.

- **Löschen** – Das schädliche Objekt löschen. Vor dem Löschen wird eine Sicherungskopie des Objekts angelegt, um bei Bedarf das Objekt oder ein Infektionsbild wiederherstellen zu können.

- **Überspringen** - Der Zugriff auf das Objekt wird gesperrt. Keine Aktion mit dem Objekt vornehmen, sondern nur Informationen darüber im Bericht aufzeichnen.

  Sie können später aus dem Berichtsfenster zur Verarbeitung von übersprungenen schädlichen Objekten zurückkehren (für Objekte, die in E-Mails gefunden wurden, steht die Option zur aufgeschobenen Verarbeitung nicht zur Verfügung).

Um die ausgewählte Aktion auf alle Objekte mit dem gleichen Status anzuwenden, die während der laufenden Sitzung der Schutzkomponente oder Aufgabe gefunden werden, aktivieren Sie das Kontrollkästchen ☑ **In allen ähnlichen Fällen anwenden**. Als laufende Sitzung gelten die Arbeitszeit einer Komponente ab dem Zeitpunkt ihres Starts bis zum Moment des Ausschaltens oder Neustarts des Programms, sowie die Ausführungszeit einer Untersuchungsaufgabe ab dem Start bis zum Abschluss.

DESINFEKTION DES OBJEKTS IST NICHT MÖGLICH

In bestimmten Fällen ist die Desinfektion eines schädlichen Objekts nicht möglich. So kann eine Datei beispielsweise so stark beschädigt sein, dass es nicht möglich ist, den schädlichen Code daraus zu löschen und sie vollständig wiederherzustellen. Außerdem ist die Desinfektionsprozedur nicht einige Arten von schädlichen Objekten wie z.B. Trojaner-Programme nicht anwendbar.

In solchen Fällen erscheint auf dem Bildschirm eine spezielle Meldung, die folgende Informationen enthält:

- Art der Bedrohung (beispielsweise *Virus*, *trojanisches Programm*) und Name des schädlichen Objekts, der seiner Bezeichnung in der Viren-Enzyklopädie von Kaspersky Lab entspricht. Der Name des schädlichen Objekts besitzt die Form eines Links zu der Ressource http://www.viruslist.com/de, auf der Sie ausführliche Informationen darüber erhalten können, welche Art von Bedrohung auf Ihrem Computer gefunden wurde.

- Vollständiger Name und Pfad des schädlichen Objekts.

Ihnen wird angeboten, eine der folgenden Aktionen für das Objekt auszuwählen:

- **Löschen** – Das schädliche Objekt löschen. Vor dem Löschen wird eine Sicherungskopie des Objekts angelegt, um bei Bedarf das Objekt oder ein Infektionsbild wiederherstellen zu können.

- **Überspringen** – Der Zugriff auf das Objekt wird gesperrt. Keine Aktion mit dem Objekt vornehmen, sondern nur Informationen darüber im Bericht protokollieren.

  Sie können später aus dem Berichtsfenster zur Verarbeitung von übersprungenen schädlichen Objekten zurückkehren (für Objekte, die in E-Mails gefunden wurden, steht die Option zur aufgeschobenen Verarbeitung nicht zur Verfügung).

Damit die ausgewählte Aktion auf alle Objekte mit dem gleichen Status angewendet wird, die während der laufenden Sitzung der Schutzkomponente oder Aufgabe gefunden werden, aktivieren Sie das Kontrollkästchen ☑ **In allen ähnlichen Fällen anwenden**. Als laufende Sitzung gelten die Arbeitszeit einer Komponente ab dem Zeitpunkt ihres Starts bis zum Moment des Ausschaltens oder Neustarts des Programms, sowie die Ausführungszeit einer Untersuchungsaufgabe ab dem Start bis zum Abschluss.

VERDÄCHTIGES OBJEKT WURDE GEFUNDEN

Wenn von Datei-Anti-Virus oder bei einer Untersuchungsaufgabe ein Objekt gefunden wird, das den Code eines unbekannten Virus oder den modifizierten Code eines bekannten Virus enthält, erscheint eine spezielle Meldung auf dem Bildschirm.

Die Meldung enthält:

- Art der Bedrohung (beispielsweise *Virus*, *trojanisches Programm*) und Name des Objekts, der seiner Bezeichnung in der Viren-Enzyklopädie von Kaspersky Lab entspricht. Der Name des schädlichen Objekts besitzt die Form eines Links zu der Ressource http://www.viruslist.com/de, auf der Sie ausführliche Informationen darüber erhalten können, welche Art von Bedrohung auf Ihrem Computer gefunden wurde.

- Vollständiger Name und Pfad des Objekts.

Ihnen wird angeboten, eine der folgenden Aktionen für das Objekt auszuwählen:

- **Quarantäne** - Das Objekt wird in die Quarantäne verschoben. Ein Objekt unter Quarantäne zu stellen, bedeutet, es wird nicht kopiert, sondern verschoben: Das Objekt wird am ursprünglichen Speicherort oder aus einer E-

Mail-Nachricht gelöscht und im Quarantäneordner gespeichert. Die unter Quarantäne stehenden Dateien werden in einem speziellen Format gespeichert und stellen keine Gefahr dar.

Bei späteren Untersuchungen der Quarantäne mit aktualisierten Bedrohungssignaturen kann sich der Status eines Objekts ändern. Das Objekt kann beispielsweise als infiziert erkannt und mit Hilfe der aktuellen Datenbanken verarbeitet werden. Oder das Objekt erhält den Status *virenfrei* und kann wiederhergestellt werden.

- **Löschen** – Das Objekt löschen. Vor dem Löschen wird eine Sicherungskopie des Objekts angelegt, um bei Bedarf das Objekt oder ein Infektionsbild wiederherstellen zu können.

- **Überspringen** – Der Zugriff auf das Objekt wird gesperrt. Keine Aktion mit dem Objekt vornehmen, sondern nur Informationen darüber im Bericht protokollieren.

  Sie können später aus dem Berichtsfenster zur Verarbeitung von übersprungenen schädlichen Objekten zurückkehren (für Objekte, die in E-Mails gefunden wurden, steht die Option zur aufgeschobenen Verarbeitung nicht zur Verfügung).

Um die ausgewählte Aktion auf alle Objekte mit dem gleichen Status anzuwenden, die während der laufenden Sitzung der Schutzkomponente oder Aufgabe gefunden werden, aktivieren Sie das Kontrollkästchen ☑ **In allen ähnlichen Fällen anwenden**. Als laufende Sitzung gelten die Arbeitszeit einer Komponente ab dem Zeitpunkt ihres Starts bis zum Moment des Ausschaltens oder Neustarts des Programms, sowie die Ausführungszeit einer Untersuchungsaufgabe ab dem Start bis zum Abschluss.

Wenn Sie überzeugt sind, dass das gefundene Objekt ungefährlich ist, können Sie es der vertrauenswürdigen Zone hinzufügen, um zu verhindern, dass das Programm bei der Arbeit mit diesem Objekt erneut anspricht.

BEDIENUNG DES PROGRAMMS ÜBER DIE BEFEHLSZEILE

Sie können Kaspersky Anti-Virus mit Hilfe der Befehlszeile steuern.

Syntax der Befehlszeile:

```
avp.com <Befehl> [Parameter]
```

Der Zugriff auf das Programm über die Befehlszeile muss aus dem Installationsordner des Kaspersky Anti-Virus oder unter Angabe des vollständigen Pfads von avp.com erfolgen.

Als <Befehl> können Sie verwenden:

- **HELP –** Hilfe über die Befehlssyntax, Anzeige einer Befehlsliste.
- **SCAN –** Untersuchung auf das Vorhandensein schädlicher Objekte.
- **UPDATE –** Programm-Update starten.
- **ROLLBACK –** Rückgängigmachen des zuletzt durchgeführten Updates von Kaspersky Anti-Virus (die Ausführung des Befehls ist nur möglich, wenn das Kennwort eingegeben wird, das über die Programmoberfläche festgelegt wurde).
- **START –** Start einer Komponente oder einer Aufgabe.
- **STOP –** Beenden der Arbeit einer Komponente oder Aufgabe (die Ausführung des Befehls ist nur möglich, wenn das Kennwort eingegeben wird, das auf dem Interface von Kaspersky Anti-Virus festgelegt wurde).
- **STATUS –** Aktuellen Status einer Komponente oder Aufgabe auf dem Bildschirm anzeigen.
- **STATISTICS –** Die Statistik über die Arbeit einer Komponente oder einer Aufgabe auf dem Bildschirm anzeigen.
- **EXPORT –** Schutzparameter des Programms exportieren.
- **IMPORT –** Importieren von Schutzeinstellungen für Kaspersky Anti-Virus (die Ausführung des Befehls ist nur möglich, wenn das Kennwort eingegeben wird, das auf dem Interface der Anwendung festgelegt wurde).
- **ACTIVATE –** Aktivierung von Kaspersky Anti-Virus über das Internet mit Hilfe eines Aktivierungscodes.
- **ADDKEY –** Programmaktivierung mit Hilfe einer Lizenzschlüsseldatei (die Ausführung des Befehls ist nur möglich, wenn das Kennwort eingegeben wird, das über die Programmoberfläche festgelegt wurde).
- **RESTORE –** Wiederherstellung einer Datei aus der Quarantäne.
- **EXIT –** Beenden der Arbeit mit dem Programm (dieser Befehl kann nur ausgeführt werden, wenn das über die Programmoberfläche festgelegte Kennwort angegeben wird).
- **TRACE –** Anlegen einer Protokolldatei.

Jedem Befehl entspricht eine eigene Auswahl von Parametern, die für eine konkrete Komponente des Programms spezifisch sind.

IN DIESEM ABSCHNITT

ANZEIGEN DER HILFE

Zur Anzeige der Hilfe über die Syntax der Befehlzeile dient folgender Befehl:

```
avp.com [ /? | HELP ]
```

Um Hilfe über die Syntax eines konkreten Befehls zu erhalten, können Sie einen der folgenden Befehle verwenden:

```
avp.com <Befehl> /?
avp.com HELP <Befehl>
```

VIRENSUCHE

Die Befehlszeile zum Starten der Virenuntersuchung eines bestimmten Bereichs und zur Verarbeitung von schädlichen Objekten besitzt generell folgendes Aussehen:

```
avp.com SCAN [<Untersuchungsobjekt>] [<Aktion>] [<Dateitypen>] [<Ausnahmen>]
[<Berichtsparameter>] [<zusätzliche Parameter>]
```

Für die Untersuchung von Objekten können Sie auch die im Programm erstellten Aufgaben verwenden, die aus der Befehlszeile gestartet werden können. Dabei wird die Aufgabe mit den Parametern ausgeführt, die über die Oberfläche von Kaspersky Anti-Virus festgelegt wurden.

Beschreibung der Parameter:

<Untersuchungsobjekt> – Der Parameter gibt eine Liste der Objekte an, die auf das Vorhandensein von schädlichem Code untersucht werden sollen. Der Parameter kann mehrere Werte aus der folgenden Liste enthalten. Die Werte werden durch Leerzeichen getrennt.

- **<files>** - Liste mit den Pfaden der Dateien und / oder Ordner für die Untersuchung. Die Angabe des absoluten oder relativen Pfads der Datei ist zulässig. Als Trennzeichen für die Elemente der Liste dient das Leerzeichen. Kommentare:
  - Wenn der Objektname ein Leerzeichen enthält, wird er in Anführungszeichen gesetzt.
  - Wenn ein konkreter Ordner angegeben wird, werden alle darin enthaltenen Dateien untersucht.
- **/ALL** – Vollständige Untersuchung des Computers.
- **/MEMORY** – Objekte des Arbeitsspeichers.
- **/STARTUP** – Autostart-Objekte.
- **/MAIL** – Mail-Datenbanken.
- **/REMDRIVES** – Alle Wechseldatenträger.
- **/FIXDRIVES** – Alle lokalen Laufwerke.
- **/NETDRIVES** – Alle Netzlaufwerke.
- **/QUARANTINE** – Objekte in Quarantäne.
- **/@:<filelist.lst>** – Pfad der Datei mit einer Liste der Objekte und Ordner, die untersucht werden sollen. Die Datei muss das Textformat besitzen. Jedes Untersuchungsobjekt muss in einer separaten Zeile stehen. Die Angabe des absoluten oder relativen Pfads der Datei ist zulässig. Der Pfad wird mit Anführungszeichen angegeben, wenn er ein Leerzeichen enthält.

<Aktion> – Der Parameter bestimmt die Aktionen mit einem schädlichen Objekt, das während der Untersuchung gefunden wird. Wenn der Parameter nicht angegeben wird, wird standardmäßig die Aktion ausgeführt, die dem Wert **/i2** entspricht. Folgende Werte sind möglich:

- **/i0** – Keine Aktion ausführen, nur Informationen im Bericht protokollieren.
- **/i1** – Infizierte Objekte desinfizieren; wenn die Desinfektion nicht möglich ist – überspringen.
- **/i2** – Infizierte Objekte desinfizieren; wenn die Desinfektion nicht möglich ist – löschen; infizierte Objekte aus Containern (zusammengesetzten Objekten) nicht löschen; Container mit ausführbarer Kopfzeile (sfx-Archive) löschen. Diese Aktion wird standardmäßig verwendet.
- **/i3** – Infizierte Objekte desinfizieren; wenn die Desinfektion nicht möglich ist – löschen; Container-Objekte vollständig löschen, wenn die darin enthaltenen infizierten Dateien nicht gelöscht werden können.
- **/i4** – Infizierte Objekte löschen; Container-Objekte vollständig löschen, wenn die darin enthaltenen infizierten Dateien nicht gelöscht werden können.
- **/i8** – Beim Fund eines infizierten Objekts den Benutzer nach der Aktion fragen.
- **/i9** – Den Benutzer nach der Aktion fragen, wenn die Untersuchung abgeschlossen wird.

<Dateitypen> – Der Parameter bestimmt die Typen der Dateien, die der Virenuntersuchung unterzogen werden. Wenn der Parameter nicht angegeben wird, werden standardmäßig nur infizierbare Dateien nach ihrem Inhalt untersucht. Folgende Werte sind möglich:

- **/fe** – Nur infizierbare Dateien nach Erweiterung untersuchen.
- **/fi** – Nur infizierbare Dateien nach Inhalt untersuchen.
- **/fa** – Alle Dateien untersuchen.

<Ausnahmen> – Der Parameter bestimmt die Objekte, die von der Untersuchung ausgeschlossen werden sollen. Der Parameter kann mehrere Werte aus der folgenden Liste enthalten. Die Werte werden durch Leerzeichen getrennt.

- **/e:a** – Archive nicht untersuchen.
- **/e:b** – Mail-Datenbanken nicht untersuchen.
- **/e:m** – E-Mail-Nachrichten im Format plain text nicht untersuchen.
- **/e:<mask>** – Objekte nach Maske nicht untersuchen.
- **/e:<seconds>** – Objekte überspringen, deren Untersuchung länger dauert, als der durch den Parameter **<seconds>** angegebene Zeitraum.

<Berichtsparameter> – Der Parameter bestimmt das Format des Berichts über die Untersuchungsergebnisse. Die Angabe des absoluten oder relativen Pfads der Datei ist zulässig. Wenn der Parameter nicht angegeben wird, werden die Untersuchungsergebnisse auf dem Bildschirm angezeigt, alle Ereignisse werden angezeigt.

- **/R:<report_file>** – Nur wichtige Ereignisse in der angegebenen Berichtsdatei protokollieren.
- **/RA:<report_file>** – Alle wichtigen Ereignisse in der angegebenen Berichtsdatei protokollieren.

<zusätzliche Parameter> – Parameter, der die Verwendung von Technologien zur Virenuntersuchung und der Konfigurationsdatei festlegt.

- **/iChecker=**<on|off> – Verwendung der Technologie iChecker aktivieren / deaktivieren.
- **/iChecker=**<on|off> – Verwendung der Technologie iSwift aktivieren / deaktivieren.
- **/C: <Name_der_Konfigurationsdatei> –** Bestimmt den Pfad der Konfigurationsdatei, in der die Parameter für die Arbeit des Programms bei der Untersuchung enthalten sind. Die Angabe des absoluten oder relativen Pfads der Datei ist zulässig. Wenn der Parameter nicht angegeben wird, werden die Werte verwendet, die über die Programmoberfläche festgelegt wurden.

Beispiele:

- *Untersuchung des Arbeitsspeichers, der Autostart-Objekte, der Maildatenbanken sowie der Ordner My Documents, Program Files und der Datei test.exe:*

```
avp.com SCAN /MEMORY /STARTUP /MAIL "C:\Documents and Settings\All Users\My Documents"
"C:\Program Files" "C:\Downloads\test.exe"
```

- *Untersuchung der Objekte, deren Liste in der Datei object2scan.txt angegeben ist. Für die Arbeit soll die Konfigurationsdatei scan_setting.txt verwendet werden. Über die Untersuchungsergebnisse soll ein Bericht erstellt werden, in dem alle Ereignisse aufgezeichnet werden:*

```
avp.com SCAN /MEMORY /@:objects2scan.txt /C:scan_settings.txt /RA:scan.log
```

Beispiel für die Konfigurationsdatei:

```
/MEMORY /@:objects2scan.txt /C:scan_settings.txt /RA:scan.log
```

PROGRAMM-UPDATE

Der Befehl für das Update der Programm-Module und Bedrohungssignaturen von Kaspersky Anti-Virus besitzt folgende Syntax:

```
avp.com UPDATE [<Updatequelle>] [/APP=<on|off>] [<Berichtsparameter>]
[<erweiterte_Einstellungen>]
```

Beschreibung der Parameter:

<Updatequelle> – HTTP-, FTP-Server oder Netzwerkordner für den Download von Updates. Wenn der Pfad nicht angegeben wird, wird die Updatequelle aus den Parametern des Diensts für das Programm-Update übernommen.

/APP=<on|off> – Update der Programm-Module aktivieren / deaktivieren.

<Berichtsparameter> – Der Parameter bestimmt das Format des Berichts über die Untersuchungsergebnisse. Die Angabe des absoluten oder relativen Pfads der Datei ist zulässig. Wenn der Parameter nicht angegeben wird, werden die Untersuchungsergebnisse auf dem Bildschirm angezeigt, alle Ereignisse werden angezeigt. Folgende Werte sind möglich:

- **/R:<report_file>** – Nur wichtige Ereignisse in der angegebenen Berichtsdatei protokollieren.
- **/RA:<report_file>** – Alle wichtigen Ereignisse in der angegebenen Berichtsdatei protokollieren.

<zusätzliche Parameter> – Parameter, der die Verwendung von der Konfigurationsdatei festlegt.

> **/C: <Name_der_Konfigurationsdatei> –** Bestimmt den Pfad der Konfigurationsdatei, in der die Parameter für die Arbeit des Programms bei der Untersuchung enthalten sind. Die Angabe des absoluten oder relativen Pfads der Datei ist zulässig. Wenn der Parameter nicht angegeben wird, werden die Werte verwendet, die über die Programmoberfläche festgelegt wurden.

Beispiele:

- *Update der Programm-Datenbanken, alle Ereignisse im Bericht protokollieren:*

```
avp.com UPDATE /RA:avbases_upd.txt
```

- *Module von Kaspersky Anti-Virus aktualisieren und dabei die Parameter der Konfigurationsdatei updateapp.ini verwenden:*

```
avp.com UPDATE /APP=on /C:updateapp.ini
```

ROLLBACK ZUM VORHERIGEN UPDATE

Befehlssyntax:

```
avp.com ROLLBACK </password=<Kennwort>> [<Berichtsparameter>]
```

Beschreibung der Parameter:

</password=<Kennwort>> – Das über die Programmoberfläche festgelegte Kennwort . Der Befehl ROLLBACK wird nur ausgeführt, wenn das Kennwort eingegeben wird.

<Berichtsparameter> – Parameter, der das Format des Berichts über die Untersuchungsergebnisse bestimmt. Die Angabe des absoluten und relativen Pfads der Datei ist zulässig. Wenn der Parameter nicht angegeben wird, werden die Untersuchungsergebnisse auf dem Bildschirm angezeigt, alle Ereignisse werden angezeigt.

- **/R:<report_file>** – Nur wichtige Ereignisse in der angegebenen Berichtsdatei protokollieren.
- **/RA:<report_file>** – Alle wichtigen Ereignisse in der angegebenen Berichtsdatei protokollieren. Die Angabe des absoluten oder relativen Pfads der Datei ist zulässig. Wenn der Parameter nicht angegeben wird, werden die Untersuchungsergebnisse auf dem Bildschirm angezeigt, alle Ereignisse werden angezeigt.

Beispiel:

```
avp.com ROLLBACK/password=123/RA:rollback.txt
```

STARTEN / BEENDEN VON DATEI-ANTI-VIRUS ODER EINER AUFGABE

Syntax des START-Befehls:

```
avp.com START <Profil|Aufgabenname> [Berichtsparameter>]
```

Syntax des STOP-Befehls:

```
avp.com STOP <Profil|Aufgabenname> </password=<Kennwort>>
```

Beschreibung der Parameter:

</password=<Kennwort>> – Das über die Programmoberfläche festgelegte Kennwort . Der Befehl STOP wird nur ausgeführt, wenn das Kennwort eingegeben wird.

<Berichtsparameter> – Der Parameter bestimmt das Format des Berichts über die Untersuchungsergebnisse. Die Angabe des absoluten und relativen Pfads der Datei ist zulässig. Wenn der Parameter nicht angegeben wird, werden die Untersuchungsergebnisse auf dem Bildschirm angezeigt, alle Ereignisse werden angezeigt. Folgende Werte sind möglich:

- **/R:<report_file>** – Nur wichtige Ereignisse in der angegebenen Berichtsdatei protokollieren.
- **/RA:<report_file>** – Alle wichtigen Ereignisse in der angegebenen Berichtsdatei protokollieren. Die Angabe des absoluten oder relativen Pfads der Datei ist zulässig. Wenn der Parameter nicht angegeben wird, werden die Untersuchungsergebnisse auf dem Bildschirm angezeigt, alle Ereignisse werden angezeigt.

<Profil|Aufgabenname> – Einer der folgenden Werte wird angegeben:

- **Protection (RTP)** – Alle Schutzkomponenten.
- **File_Monitoring (FM)** – Datei-Anti-Virus.
- **Scan_My_Computer** – Aufgabe zur vollständigen Untersuchung des Computers.
- **Scan_Objects** – Untersuchung von Objekten.
- **Scan_Quarantine** – Quarantäne untersuchen.
- **Scan_Startup (STARTUP)** – Untersuchung von Autostart-Objekten.
- **Updater** – Updateaufgabe.
- **Rollback** – Aufgabe Rollback des Updates.

Die aus der Befehlszeile gestarteten Komponenten und Aufgaben werden mit den Parametern ausgeführt, die über die Programmoberfläche festgelegt wurden.

Beispiele:

- *Um Datei-Anti-Virus zu aktivieren, geben Sie in der Befehlszeile ein:*

```
avp.com START FM
```

- *Um die Aufgabe zur vollständigen Untersuchung zu beenden, geben Sie in der Befehlszeile ein:*

avp.com STOP SCAN_MY_COMPUTER /password=<Kennwort>

STATISTIK ÜBER DIE ARBEIT EINER KOMPONENTE ODER AUFGABE

Syntax des STATUS-Befehls:

```
avp.com STATUS <Profil|Aufgabenname>
```

Syntax des STATISTICS-Befehls:

```
avp.com STATISTICS <Profil|Aufgabenname>
```

Beschreibung der Parameter:

<Profil|Aufgabenname> – wird einer der im Befehl START / STOP (s. S. 114) genannten Werte angegeben.

EXPORT VON SCHUTZPARAMETERN

Befehlssyntax:

```
avp.com EXPORT <Profil|Aufgabenname> <Dateiname>
```

Beschreibung der Parameter:

<Profil|Aufgabenname> – wird einer der im Befehl START / STOP (s. S. 114) genannten Werte angegeben.

<Dateiname> – Pfad der Datei, in welche die Parameter vom Programm exportiert werden. Ein absoluter oder relativer Pfad kann angegeben werden.

Beispiel:

```
avp.com EXPORT RTP RTP_settings.dat – Binärformat
avp.com EXPORT FM FM_settings.txt – Textformat
```

IMPORT VON SCHUTZPARAMETERN

Befehlssyntax:

```
avp.com IMPORT <Dateiname> </password=<Kennwort>]
```

Beschreibung der Parameter:

<Dateiname> – Pfad der Datei, in welche die Parameter vom Programm exportiert werden. Ein absoluter oder relativer Pfad kann angegeben werden.

</password=<Kennwort>> – Das über die Programmoberfläche festgelegte Kennwort .

Beispiel:

```
avp.com IMPORT settings.dat
```

PROGRAMM AKTIVIEREN

Die Aktivierung von Kaspersky Anti-Virus kann auf zwei Arten erfolgen:

- über das Internet mit Hilfe eines Aktivierungscodes (Befehl ACTIVATE)

- mit Hilfe einer Schlüsseldatei (Befehl ADDKEY).

Befehlssyntax:

```
avp.com ACTIVATE <Aktivierungscode> </password=<Kennwort>>
avp.com ADDKEY <Dateiname> </password=<Kennwort>>
```

Beschreibung der Parameter:

<Aktivierungscode> – Aktivierungscode: xxxxx-xxxxx-xxxxx-xxxxx.

<Dateiname> – Lizenzschlüsseldatei für das Programm (Endung *.key): xxxxxxxx.key.

</password=<Kennwort>> – Das über die Programmoberfläche festgelegte Kennwort .

Beispiel:

```
avp.com ACTIVATE 11AA1-11AAA-1AA11-1A111
avp.com ADDKEY 1AA111A1.key </password=<Kennwort>
```

WIEDERHERSTELLUNG EINER DATEI AUS DER QUARANTÄNE

Befehlssyntax:

```
avp.com RESTORE [/REPLACE] <Dateiname>
```

Beschreibung der Parameter:

/REPLACE – Vorhandene Datei ersetzen

<Dateiname> – Name der Datei zum Wiederherstellen.

Beispiel:

```
avp.com REPLACE C:\eicar.com
```

PROGRAMM BEENDEN

Befehlssyntax:

```
avp.com EXIT </password=<Kennwort>>
```

Beschreibung der Parameter:

</password=<Kennwort>> – Das über die Programmoberfläche festgelegte Kennwort . Der Befehl wird nur ausgeführt, wenn das Kennwort eingegeben wird.

ANLEGEN EINER PROTOKOLLDATEI

Das Anlegen einer Ablaufverfolgungsdatei kann erforderlich sein, wenn bei der Arbeit mit Kaspersky Anti-Virus Probleme auftreten, deren genaue Analyse durch die Experten des Technischen Supports notwendig ist.

Befehlssyntax:

```
avp.com TRACE [file] [on|off] [<Tracing-Niveau>]
```

Beschreibung der Parameter:

[on|off] – Anlegen einer Protokolldatei aktivieren / deaktivieren.

[file] – Tracing in Form einer Datei erstellen.

<Tracing-Niveau> – Für den Parameter kann ein Zahlenwert im Bereich von 100 (minimale Stufe, nur kritische Meldungen) bis 600 (maximale Stufe, alle Meldungen) festgelegt werden.

Bei einer Anfrage an den Technischen Support, ist die Angabe des Tracing-Niveaus erforderlich. Andernfalls gilt das Niveau 500 als empfehlenswert.

Beispiele:

- *Erstellen von Protokolldateien deaktivieren:*

```
avp.com TRACE file off
```

- *Erstellen einer Protokolldatei mit einem Tracing-Niveau von 500:*

```
avp.com TRACE file on 500
```

RÜCKGABECODES DER BEFEHLSZEILE

Die allgemeinen Codes können von einem beliebigen Befehl der Befehlszeile zurückgegeben werden. Als Rückgabecodes für Aufgaben sind die allgemeinen Codes sowie spezifische Codes für einen konkreten Aufgabentyp möglich.

Allgemeine Rückgabecodes:

- 0 – Operation wurde erfolgreich ausgeführt.
- 1 – Ungültiger Parameterwert.
- 2 – Unbekannter Fehler.
- 3 – Fehler bei Ausgabenausführung.
- 4 – Aufgabenausführung wurde abgebrochen.

Rückgabecodes für Aufgaben zur Virensuche:

- 101 – Alle gefährlichen Objekte wurden verarbeitet.
- 102 – Es wurden gefährliche Objekte gefunden.

PROGRAMM ÄNDERN, REPARIEREN ODER LÖSCHEN

Für die Deinstallation der Anwendung gibt es folgende Möglichkeiten:

- mit Hilfe des Installationsassistenten für das Programm.
- aus der Befehlszeile (s. Abschnitt "Programm über die Befehlszeile löschen" auf S. 120).
- über Kaspersky Administration Kit (s. "Handbuch zur Einführung von Kaspersky Administration Kit").
- über Domain-Gruppenaufgaben für Microsoft Windows Server 2000/2003 (s. Abschnitt "Programm löschen" auf S. 23).

IN DIESEM ABSCHNITT

PROGRAMM MIT HILFE DES INSTALLATIONSASSISTENTEN ÄNDERN, REPARIEREN ODER LÖSCHEN

Die Reparatur des Programms kann dann von Nutzen sein, wenn Sie Fehler in seiner Arbeit feststellen, die auf fehlerhafte Einstellungen oder beschädigte Programmdateien zurückgehen.

➧ *Gehen Sie folgendermaßen vor, um den ursprünglichen Programmzustand wiederherzustellen, um Komponenten von Kaspersky Anti-Virus, die bei der Erstinstallation nicht installiert wurden, zu installieren, oder um das Programm zu löschen:*

1. Legen Sie die CD mit der Programmdistribution in das CD/DVD-ROM-Laufwerk ein, wenn die Installation von dort aus erfolgte. Wenn die Installation von Kaspersky Anti-Virus aus einer anderen Quelle erfolgte (z.B. gemeinsamer Ordner, Ordner auf der Festplatte), vergewissern Sie sich, dass die Programmdistribution in diesem Ordner vorhanden ist und Sie zugriffsberechtigt sind.

2. Wählen Sie **Start** → **Programme** → **Kaspersky Anti-Virus 6.0 für Windows Server MP4** → **Ändern, Reparieren oder Löschen**.

Dadurch wird das Installationsprogramm gestartet, das die Form eines Assistenten besitzt. Im Folgenden werden die Schritte zur Reparatur, zum Ändern des Bestands der Programmkomponenten und zum Löschen des Programms ausführlich beschrieben.

SCHRITT 1. STARTFENSTER DES INSTALLATIONSPROGRAMMS

Wenn Sie alle oben beschriebenen Aktionen ausgeführt haben, die für die Reparatur oder das Ändern des Komponentenbestands erforderlich sind, wird auf dem Bildschirm das Begrüßungsfenster des Installationsprogramms für Kaspersky Anti-Virus geöffnet. Klicken Sie auf **Weiter**, um fortzufahren.

SCHRITT 2. OPERATION WÄHLEN

Auf dieser Etappe müssen Sie festlegen, welche Operation Sie mit dem Programm vornehmen möchten: Zur Auswahl stehen das Ändern des Komponentenbestands, das Wiederherstellen des ursprünglichen Zustands der installierten Komponenten oder das Löschen bestimmter Komponenten oder des ganzen Programms. Klicken Sie zum Ausführen einer Operation auf die entsprechende Schaltfläche. Die weiteren Aktionen des Installationsprogramms sind von der gewählten Operation abhängig.

Das Vorgehen beim Ändern des Komponentenbestands entspricht der benutzerdefinierten Installation des Programms, bei der Sie festlegen können, welche Komponenten installiert und welche gelöscht werden sollen.

Die Reparatur des Programms erfolgt auf Basis der installierten Komponenten. Alle Dateien der installierten Komponenten werden aktualisiert und für jede dieser Komponenten wird die **empfohlene** Sicherheitsstufe eingestellt.

Wenn die Remote-Deinstallation von Kaspersky Anti-Virus 6.0 ausgeführt wird, erfolgt kein automatischer Neustart des Servers. Es wird allerdings empfohlen, manuell einen Neustart vorzunehmen, um alle Programmkomponenten vollständig zu entfernen und die korrekte Funktion des Computers zu gewährleisten.

Beim Löschen des Programms können Sie wählen, welche Daten, die bei der Arbeit des Programms erstellt und verwendet wurden, auf Ihrem Computer gespeichert werden sollen. Um alle Daten von Kaspersky Anti-Virus zu löschen, wählen Sie die Variante **Anwendung vollständig löschen**. Um bestimmte Daten zu speichern, wählen Sie die Variante **Objekte der Anwendung speichern** und geben Sie an, welche Objekte beibehalten werden sollen:

- *Aktivierungsdaten* – Schlüsseldatei, die für die Arbeit des Programms erforderlich ist.
- *Programm-Datenbanken* – Vollständige Auswahl der Signaturen der gefährlichen Programme, Viren und anderen Bedrohungen, die zum Zeitpunkt des letzten Updates aktuell waren.
- *Backup-Objekte* – Sicherungskopien von gelöschten oder desinfizierten Objekten. Es wird empfohlen, diese Objekte zu speichern, um sie bei Bedarf später wiederherzustellen.
- *Quarantäneobjekte* – Objekte, die möglicherweise von Viren oder Virusmodifikationen infiziert sind. Solche Objekte enthalten Code, der Ähnlichkeit mit dem Code eines bekannten Virus besitzt. Allerdings lässt sich nicht sicher sagen, ob sie schädlich sind. Es wird empfohlen, diese Objekte zu speichern, weil sie sich als virenfrei erweisen oder später unter Verwendung von aktualisierten Bedrohungssignaturen desinfiziert werden können.
- *Schutzparameter* – Parameterwerte für die Arbeit aller Programmkomponenten.
- *iSwift-Daten* – Datenbank, die Informationen über untersuchte Objekte des NTFS-Dateisystems enthält. Sie erlaubt die Beschleunigung der Objektuntersuchung. Bei Einsatz dieser Datenbank untersucht Kaspersky Anti-Virus nur jene Objekte, die seit der letzten Untersuchung verändert wurden.

Wenn zwischen der Deinstallation einer Version von Kaspersky Anti-Virus und der Installation einer anderen Version ein relativ großer Zeitraum liegt, wird davon abgeraten, die aus der vorherigen Programminstallation stammende iSwift-Datenbank zu verwenden. In der Zwischenzeit kann ein gefährliches Programm auf den Computer gelangt sein, dessen schädliche Aktionen bei Verwendung dieser Datenbank nicht erkannt werden, was zu einer Infektion des Computers führen kann.

Klicken Sie auf die Schaltfläche **Weiter**, um die gewählte Operation zu starten. Der Prozess zum Kopieren der notwendigen Dateien auf Ihren Computer oder zum Löschen der ausgewählten Komponenten und Daten wird gestartet.

SCHRITT 3. OPERATION ZUM REPARIEREN, ÄNDERN ODER LÖSCHEN DES PROGRAMMS ABSCHLIEßEN

Der Fortschritt des Prozesses zum Reparieren, Ändern oder Löschen wird auf dem Bildschirm dargestellt. Danach erfolgt ein Hinweis auf den Abschluss der Operation.

Die Deinstallation macht in der Regel einen Neustart des Computers erforderlich, um Änderungen im System zu berücksichtigen. Auf dem Bildschirm erscheint eine Anfrage für den Neustart des Computers. Klicken Sie auf die Schaltfläche **Ja**, um sofort einen Neustart vorzunehmen. Um den Computer später auf Befehl neu zu starten, klicken Sie auf **Nein**.

PROGRAMM ÜBER DIE BEFEHLSZEILE LÖSCHEN

- *Um Kaspersky Anti-Virus 6.0 für Windows Workstation MP4 aus der Befehlszeile zu deinstallieren, geben Sie ein:*

  `msiexec /x <Paketname>`

  Es wird ein Installationsassistent gestartet, mit dessen Hilfe Sie die Deinstallation der Anwendung vornehmen können.

- *Um die Anwendung im Silent-Modus ohne Neustart des Computers zu deinstallieren (der Neustart muss nach der Deinstallation manuell ausgeführt werden), geben Sie ein:*

  `msiexec /x <Paketname> /qn`

- *Um die Anwendung im Silent-Modus mit anschließendem Neustart des Computers zu deinstallieren, geben Sie ein:*

  `msiexec /x <Paketname> ALLOWREBOOT=1 /qn`

Wenn bei der Programminstallation ein Kennwort für die Deinstallation festgelegt wurde, muss beim Entfernen des Produkts das Kennwort angegeben werden, andernfalls wird die Deinstallation nicht ausgeführt.

- *Um die Anwendung unter Angabe des für die Programmdeinstallation erforderlichen Kennworts zu deinstallieren, geben Sie ein:*

  `msiexec /x <Paketname> KLUNINSTPASSWD=******` – für die Programmdeinstallation im interaktiven Modus.

  `msiexec /x <Paketname> KLUNINSTPASSWD=****** /qn` – für die Programmdeinstallation im Silent-Modus.

VERWALTUNG DER ANWENDUNG ÜBER KASPERSKY ADMINISTRATION KIT

Kaspersky Administration Kit wird in Computernetzwerken von Unternehmen eingesetzt und dient der zentralisierten Lösung der wichtigsten Verwaltungsaufgaben in Antiviren-Sicherheitssystemen, die auf Anwendungen der Produkte von Kaspersky Open Space Security basieren. Kaspersky Administration Kit unterstützt die Arbeit in allen Netzwerkkonfigurationen, die das Protokoll TCP/IP verwenden.

Die Anwendung ist bestimmt für Administratoren von Firmennetzen sowie für Mitarbeiter, die für den Antiviren-Schutz von Computern in Organisationen verantwortlich sind.

Kaspersky Anti-Virus 6.0 für Windows Server MP4 ist ein Produkt von Kaspersky Lab. Es kann über das eigene Interface der Anwendung, über die Befehlszeile (diese Methoden werden in diesem Handbuch weiter oben beschrieben) oder mit der Anwendung Kaspersky Administration Kit verwaltet werden (wenn der Computer zu einem zentralen Fernverwaltungssystem gehört).

Gehen Sie folgendermaßen vor, um Kaspersky Anti-Virus über Kaspersky Administration Kit zu verwalten:

- Richten Sie im Netzwerk einen *Administrationsserver* ein.
- Installieren Sie die *Administrationskonsole* am Arbeitsplatz des Administrators (Details siehe Handbuch zur Einführung von "Kaspersky Administration Kit").
- Installieren Sie auf den Netzwerkcomputern das Programm Kaspersky Anti-Virus und den *Administrationsagenten* (gehört zu Kaspersky Administration Kit). Eine genaue Beschreibung der Remote-Installation des Installationspakets von Kaspersky Anti-Virus auf Netzwerkcomputern finden Sie im Handbuch zur Einführung von "Kaspersky Administration Kit".

Beenden Sie die Administrationskonsole, bevor Sie das Upgrade des Verwaltungs-Plug-ins für Kaspersky Anti-Virus über Kaspersky Administration Kit vornehmen.

Die Verwaltung der Anwendung über Kaspersky Administration Kit erfolgt mit der Administrationskonsole (s. Abb. unten). Sie stellt ein standardmäßiges Interface dar, das in MMC integriert ist, und bietet dem Administrator folgende Funktionen:

- Remote-Installation von Kaspersky Anti-Virus und des *Administrationsagenten* auf den Netzwerkcomputern.
- Remote-Konfiguration von Kaspersky Anti-Virus auf den Netzwerkcomputern.
- Aktualisierung der Datenbanken und Module von Kaspersky Anti-Virus.
- Verwaltung der Lizenzen für Kaspersky Anti-Virus auf den Netzwerkcomputern.

- Anzeige von Informationen über die Arbeit der Anwendung auf den Client-Computern.

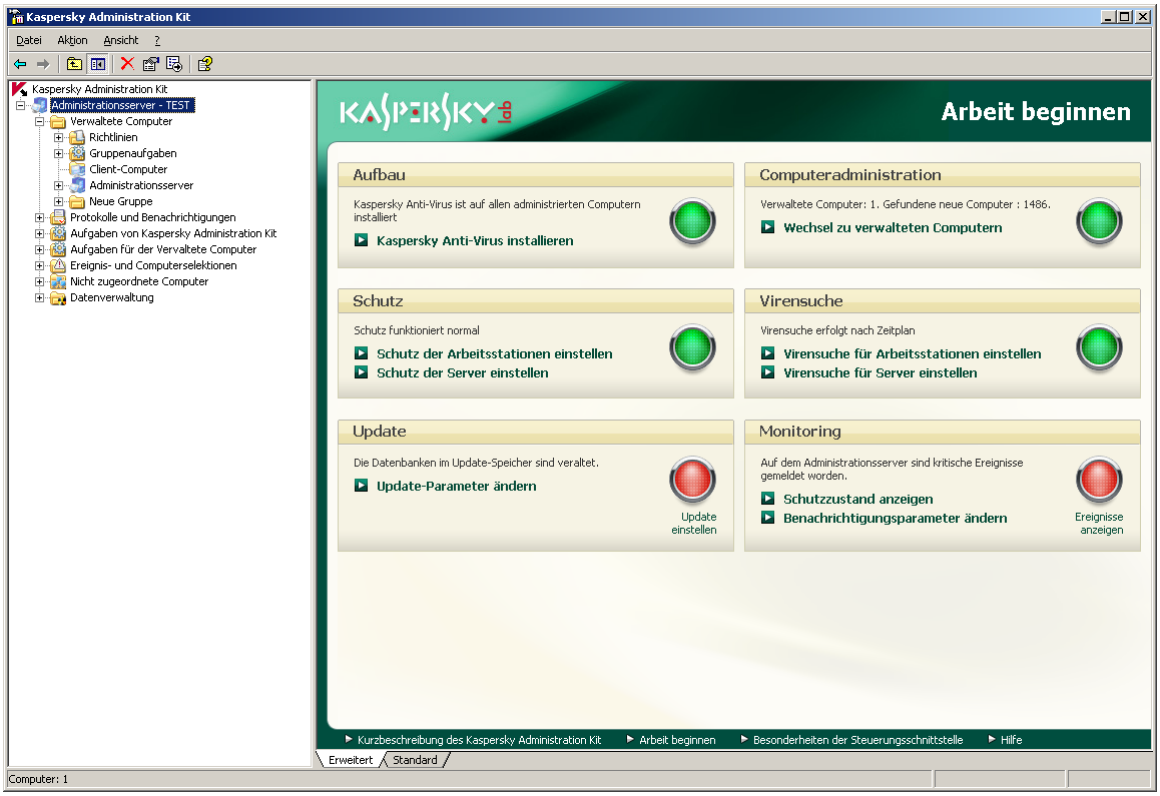


Abbildung 11. Administrationskonsole von Kaspersky Administration Kit.

Das Aussehen des Hauptfensters von Kaspersky Administration Kit kann in Abhängigkeit des auf Ihrem Computer verwendeten Betriebssystem variieren.

Bei der Arbeit über Kaspersky Administration Kit verwaltet der Administrator die Anwendung mit Hilfe der Parameter für die Anwendung, für Richtlinien und für Aufgaben.

Eine *Aufgabe* ist eine Aktion, die einen Namen besitzt und von der Anwendung ausgeführt werden kann. Aufgaben werden nach den auszuführenden Funktionen in *Typen* unterteilt: Untersuchungsaufgabe, Aufgabe zum Programm-Update oder zum Rollback von Updates, Aufgabe zur Installation einer Schlüsseldatei.

Jeder Aufgabe entspricht bei ihrer Ausführung eine Auswahl von Funktionsparametern der Anwendung. Eine Auswahl von Funktionsparametern, die für alle Typen von Aufgaben einheitlich ist, sind die *Anwendungsparameter*. Die Funktionsparameter der Anwendung, die für jeden Typ der Aufgaben spezifisch sind, bilden die *Aufgabenparameter*. Anwendungsparameter und Aufgabenparameter überschneiden sich nicht.

Eine Besonderheit der zentralisierten Verwaltung besteht darin, dass die Netzwerkcomputer in Gruppen organisiert sind, die durch Gruppenrichtlinien verwaltet werden.

Eine *Richtlinie* ist eine gruppenspezifische Auswahl von Parametern für die Anwendungsfunktion sowie eine Auswahl von Beschränkungen für das Ändern dieser Parameter, die sich auf die Konfiguration der Anwendung oder einer Aufgabe auf einem bestimmten Client-Computer beziehen. Eine Richtlinie umfasst die Parameter zur vollständigen Konfiguration der gesamten Anwendungsfunktionalität, unter Ausnahme spezifischer Parameter für konkrete Aufgabenexemplare. Als spezifisch gelten zum Beispiel die Zeitplanparameter.

Eine Richtlinie umfasst folgende Parameter:

- Parameter, die für alle Aufgabentypen gelten, auch Anwendungsparameter genannt.
- Parameter, die für alle Exemplare der Aufgaben jedes Typs gelten – der Großteil der Aufgabenparameter.

Das bedeutet, dass eine Richtlinie für Kaspersky Anti-Virus, zu dem Schutzaufgaben und Untersuchungsaufgaben gehören, alle erforderlichen Parameter für die Konfiguration der Anwendung bei der Ausführung beider Aufgabentypen umfasst, aber beispielsweise den Startzeitplan dieser Aufgaben oder die Parameter für den Untersuchungsbereich nicht berücksichtigt.

IN DIESEM ABSCHNITT

ANWENDUNGSSTEUERUNG

Kaspersky Administration Kit bietet die Möglichkeit, den Start und das Beenden von Kaspersky Anti-Virus auf einem einzelnen Client-Computer fernzusteuern. Außerdem kann die Konfiguration gemeinsamer Funktionsparameter der Anwendung entfernt verwaltet werden (z.B. Computerschutz aktivieren und deaktivieren, Parameter für Berichte und Speicher anpassen).

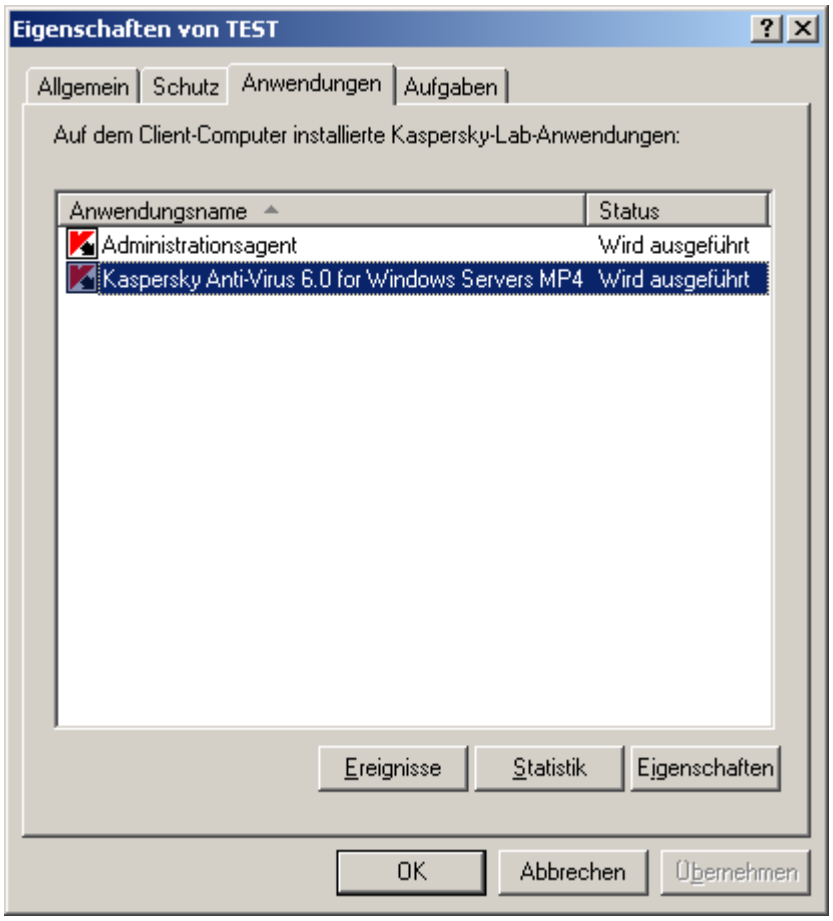


*Abbildung 12. Fenster mit Eigenschaften eines Client-Computers. Registerkarte **Programme***

➡ *Gehen Sie folgendermaßen vor, um die Anwendungsparameter anzuzeigen oder anzupassen:*

1. Öffnen Sie die Administrationskonsole von Kaspersky Administration Kit.
2. Öffnen Sie im Ordner **Verwaltete Computer** den Ordner der Gruppe, zu der der Client-Computer gehört.

3. Öffnen Sie in der gewählten Gruppe den Unterordner **Client-Computer** und wählen Sie im Detailfenster einen Computer aus, für den die Anwendungsparameter geändert werden sollen.

4. Verwenden Sie im Kontextmenü den Befehl **Eigenschaften** oder den entsprechenden Punkt im Menü **Aktion**, um das Eigenschaftenfenster des Client-Computers zu öffnen.

5. Das Eigenschaftenfenster des Client-Computers zeigt auf der Registerkarte **Anwendungen** eine vollständige Liste aller auf dem Client-Computer installierten Kaspersky-Lab-Anwendungen. Wählen Sie das Programm **Kaspersky Anti-Virus 6.0 für Windows Server MP4** aus.

   Unter der Liste der Anwendungen befinden sich Schaltflächen mit folgenden Funktionen:

   - Anzeige einer Liste mit Ereignissen bei der Arbeit der Anwendung, die auf dem Client-Computer eingetreten sind und auf dem Administrationsserver registriert wurden.
   - Anzeige von aktuellen statistischen Informationen über die Arbeit der Anwendung.
   - Programmparameter anpassen (s. S. 125).

PROGRAMM STARTEN UND BEENDEN

Der Start und das Beenden von Kaspersky Anti-Virus 6.0 auf einem entfernten Client-Computer erfolgen aus dem Eigenschaftenfenster der Anwendung (s. Abb. unten).

Der obere Bereich des Fensters enthält folgende Angaben über die installierte Anwendung: Name, Version, Installationsdatum, Status (ob die Anwendung auf dem lokalen Computer gestartet oder beendet wurde), Informationen über den Zustand der Datenbanken mit den Bedrohungssignaturen.

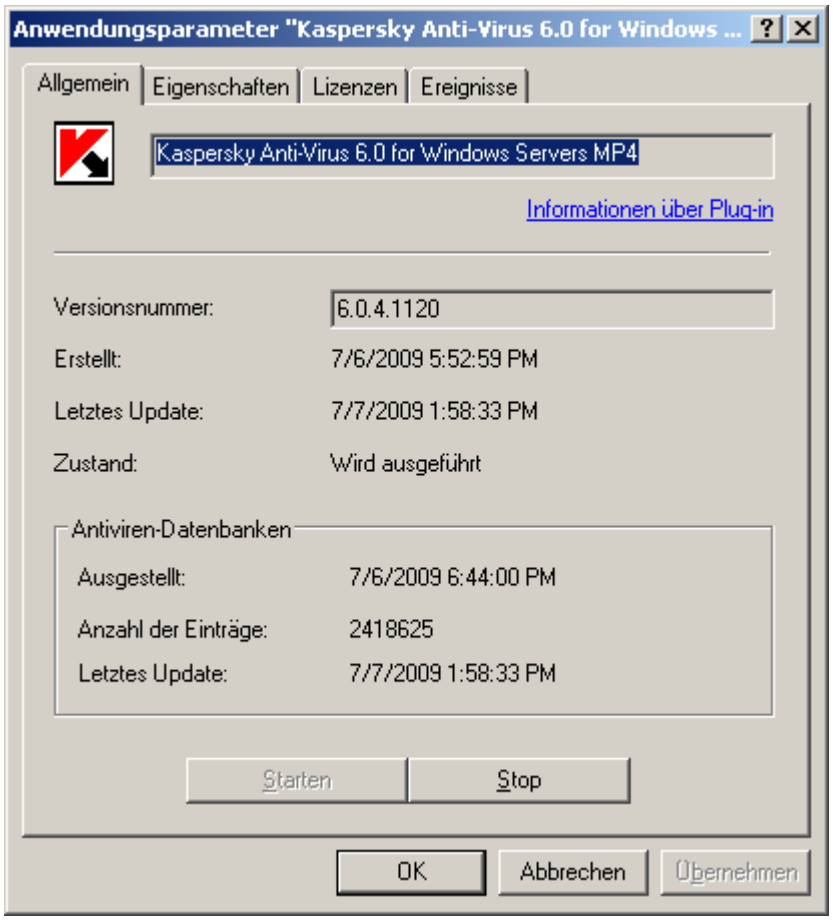


*Abbildung 13. Eigenschaftenfenster der Anwendung. Registerkarte **Allgemein***

Gehen Sie folgendermaßen vor, um die Anwendung auf einem Remote-Computer zu beenden oder zu starten:

1. Öffnen Sie das Eigenschaftenfenster des Client-Computers (s. S. 123) auf der Registerkarte **Programme**.
2. Wählen Sie die Anwendung **Kaspersky Anti-Virus 6.0 für Windows Server MP4** und klicken Sie auf die Schaltfläche **Eigenschaften**.
3. Klicken Sie im folgenden Fenster mit den Eigenschaften der Anwendung auf der Registerkarte **Allgemein** auf die Schaltfläche **Beenden**, um die Anwendung zu beenden, oder auf **Starten**, um sie zu starten.

PROGRAMMPARAMETER ANPASSEN

Die Anwendungsparameter werden im Eigenschaftenfenster der Anwendung auf der Registerkarte **Einstellungen** angezeigt und geändert (s. Abb. unten). Alle übrigen Registerkarten sind für die Anwendung Kaspersky Administration Kit standardmäßig und werden im entsprechenden Handbuch ausführlich beschrieben.

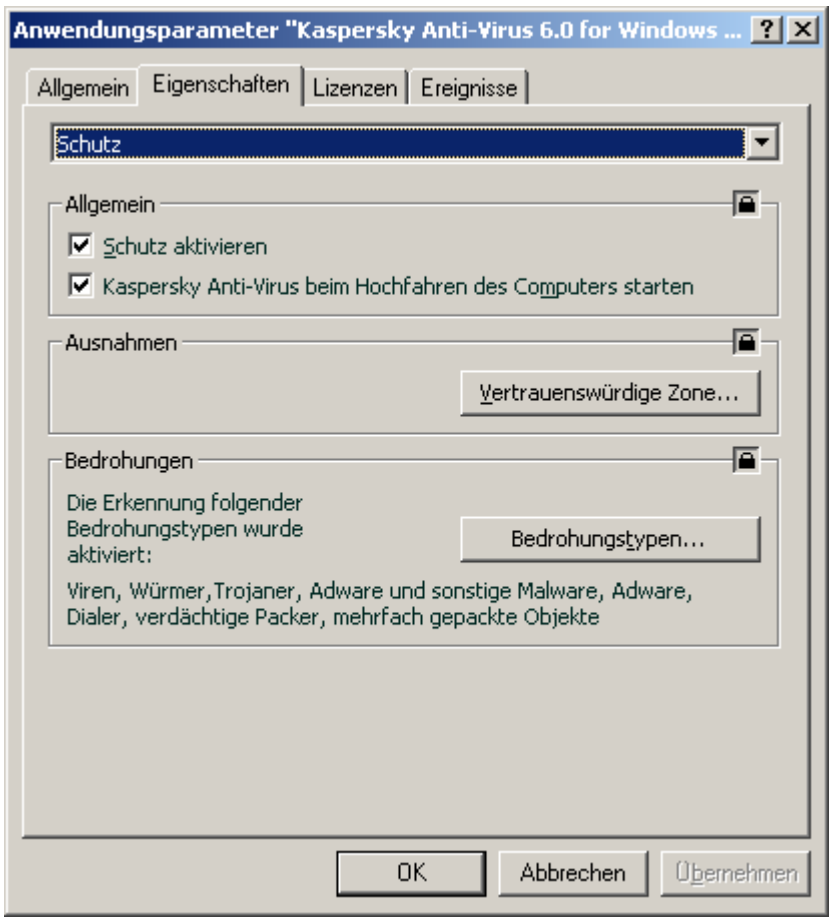


*Abbildung 14. Eigenschaftenfenster der Anwendung. Registerkarte **Einstellungen***

Wenn für eine Anwendung eine Richtlinie erstellt wurde (auf S. 134), durch die das Ändern bestimmter Parameter verboten wird, dann können diese beim Anpassen der Anwendungsparameter nicht geändert werden.

Gehen Sie folgendermaßen vor, um die Anwendungsparameter anzuzeigen oder anzupassen:

1. Öffnen Sie das Eigenschaftenfenster des Client-Computers (s. S. 123) auf der Registerkarte **Programme**.
2. Wählen Sie die Anwendung **Kaspersky Anti-Virus 6.0 für Windows Server MP4** und klicken Sie auf die Schaltfläche **Eigenschaften**.

3. Im folgenden Fenster mit den Eigenschaften der Anwendung auf der Registerkarte **Einstellungen** können Sie folgende Parameter anpassen: generelle Funktionsparameter für Kaspersky Anti-Virus, Parameter für Berichte und Speicher, sowie Netzwerkparameter. Wählen Sie dazu aus der Dropdown-Liste im oberen Bereich des Fensters den erforderlichen Wert aus und nehmen Sie die Einstellungen vor.

SIEHE AUCH

SPEZIFISCHE PARAMETER ANPASSEN

Bei der Verwaltung von Kaspersky Anti-Virus über Kaspersky Administration Kit können Sie den Modus für die Interaktion zwischen Anwendung und Benutzer aktivieren oder deaktivieren, das Aussehen der Anwendung anpassen und die Informationen zur technischen Unterstützung ändern. Diese Parameter werden im Eigenschaftenfenster der Anwendung angepasst (s. Abb. unten).

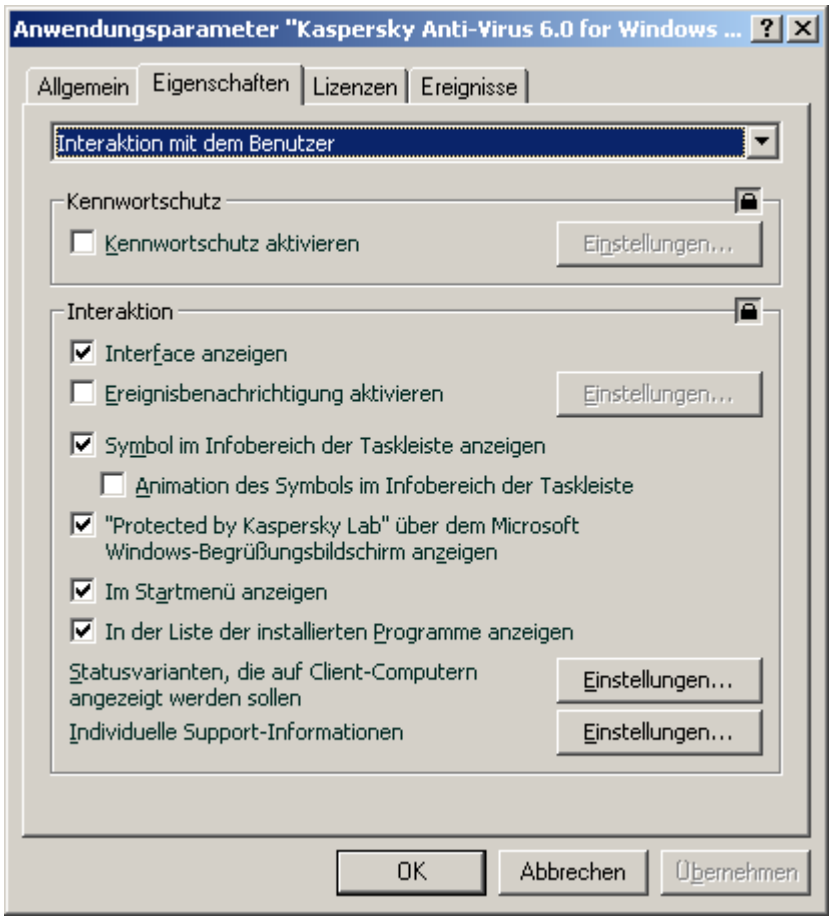


Abbildung 15. Eigenschaftenfenster der Anwendung. Spezifische Parameter anpassen

Um Kaspersky Anti-Virus mit Hilfe eines Kennworts vor unberechtigtem Zugriff zu schützen, aktivieren Sie das Kontrollkästchen **Kennwortschutz aktivieren**, klicken Sie auf die Schaltfläche **Einstellungen** und geben Sie im folgenden Fenster ein Kennwort und den Bereich an, für den die Zugriffsbeschränkung gelten soll.

Um zu verhindern, dass das Programm unerlaubterweise von dem lokalen Computer gelöscht wird, aktivieren Sie das Kontrollkästchen **Schutz vor Deinstallation aktivieren**. Geben Sie im Fenster, das mit der Schaltfläche **Einstellungen** geöffnet wird, das Kennwort für die Deinstallation an und bestätigen Sie es.

Um Kaspersky Anti-Virus mit Hilfe eines Kennworts vor unberechtigtem Zugriff zu schützen, aktivieren Sie das Kontrollkästchen **Kennwortschutz aktivieren**, klicken Sie auf die Schaltfläche **Einstellungen** und geben Sie im folgenden Fenster ein Kennwort und den Bereich an, für den die Zugriffsbeschränkung gelten soll.

Um zu verhindern, dass das Programm unerlaubterweise von dem lokalen Computer gelöscht wird, aktivieren Sie das Kontrollkästchen **Schutz vor Deinstallation aktivieren**. Geben Sie im Fenster, das mit der Schaltfläche **Einstellungen** geöffnet wird, das Kennwort für die Deinstallation an und bestätigen Sie es.

Im Block **Interaktion** können Sie die Parameter für die Interaktion zwischen Benutzer und Interface von Kaspersky Anti-Virus festlegen:

- Wenn das Kontrollkästchen **Interaktion mit Interface verbieten** aktiviert ist, sieht ein Benutzer, der auf dem Remote-Computer arbeitet, das Symbol und die Popupmeldungen von Kaspersky Anti-Virus. Außerdem kann er in Ereignismeldungen über die erforderlichen Aktionen entscheiden. Zur Deaktivierung des interaktiven Programmmodus mussen Sie das Häkchen entfernen. Wenn der Benutzer nicht bemerken soll, dass das Programm auf seinem Computer installiert ist, aktivieren Sie das Kontrollkästchen Vorhandensein des installierten Programms vollständig verbergen.

- Im Fenster **Ansicht**, das mit der Schaltfläche **Einstellungen** geöffnet wird, können Sie die Informationen über den technischen Support für Benutzer ändern, die im Fenster **Support** für Kaspersky Anti-Virus angezeigt werden.

  Um die Informationen zu ändern, geben Sie im oberen Feld den gewünschten Text über den angebotenen Support ein. Die Reihenfolge der Links kann mit Hilfe der Schaltflächen **Nützliche Links** des Fensters **Support** angezeigt werden. Dieses Fenster wird über den Link **Support** im Hauptfenster von Kaspersky Anti-Virus geöffnet.

  Zum Ändern der Liste dienen die Schaltflächen **Hinzufügen**, **Ändern** und **Löschen**. Kaspersky Anti-Virus fügt einen neuen Link am Anfang der Liste hinzu. Die Reihenfolge der Links kann mit Hilfe der Schaltflächen **Aufwärts** und **Abwärts** geändert werden.

  Wenn das Fenster keine Daten enthält, können die standardmäßig angegebenen Informationen über den technischen Support nicht geändert werden.

Im Block **Status der Anwendung** können Sie die Status der Anwendung angeben, die im Hauptfenster von Kaspersky Anti-Virus angezeigt werden sollen. Klicken Sie dazu auf die Schaltfläche **Einstellungen** und aktivieren Sie in dem sich öffnenden Fenster die Kontrollkästchen neben den erforderlichen Sicherheitsstatusanzeigen. In diesem Fenster können Sie die Prüfungsabstände für die Programm-Datenbanken angeben.

Im Block **Ansicht** können Sie die Parameter für den interaktiven Funktionsmodus von Kaspersky Anti-Virus auf einem Remote-Computer anpassen: Anzeige einer Schutzmeldung über dem Microsoft Windows-Begrüßungsbildschirm, Animation des Symbols für Kaspersky Anti-Virus im Infobereich der Taskleiste, Anzeige von Meldungen über Ereignisse, die bei der Arbeit des Programms eintreten (z.B. Fund eines gefährlichen Objekts).

Wenn für eine Anwendung eine Richtlinie erstellt wurde (s. S. 134), durch die das Ändern bestimmter Parameter verboten wird, dann können diese beim Anpassen der Anwendungsparameter nicht geändert werden.

Gehen Sie folgendermaßen vor, um die spezifischen Anwendungsparameter anzuzeigen oder anzupassen:

1. Öffnen Sie das Eigenschaftenfenster des Client-Computers (s. S. 123) auf der Registerkarte **Programme**.

2. Wählen Sie die **Anwendung** Kaspersky Anti-Virus 6.0 für Windows Server MP4 und klicken Sie auf die Schaltfläche **Eigenschaften**.

3. Wählen Sie im Eigenschaftenfenster der Anwendung auf der Registerkarte **Einstellungen** aus der Dropdown-Liste im oberen Bereich des Fensters den Punkt **Interaktion mit dem Benutzer und nehmen Sie die Einstellungen** vor.

AUFGABEN VERWALTEN

Dieser Abschnitt bietet Informationen über die Verwaltung von Aufgaben für Kaspersky Anti-Virus. Nähere Informationen zur Konzeption der Aufgabenverwaltung über Kaspersky Administration Kit finden Sie im entsprechenden Administratorhandbuch.

Bei der Installation der Anwendung wird für jeden Netzwerkcomputer eine bestimmte Auswahl von Systemaufgaben erstellt. Zu dieser Liste gehören Schutzaufgaben (Datei-Anti-Virus), Untersuchungsaufgaben (Vollständige Suche, Schnelle Suche) und Updateaufgaben (Update der Datenbanken und Programm-Module, Rollback des Updates).

Der Start von Systemaufgaben kann verwaltet und ihre Parameter können angepasst werden. Das Löschen dieser Aufgaben ist nicht möglich.

Außerdem können Sie eigene Aufgaben erstellen (s. S. 129), beispielsweise Aufgaben zur Virensuche, zum Update der Anwendung, zum Rollback eines Updates oder zur Installation einer Schlüsseldatei.

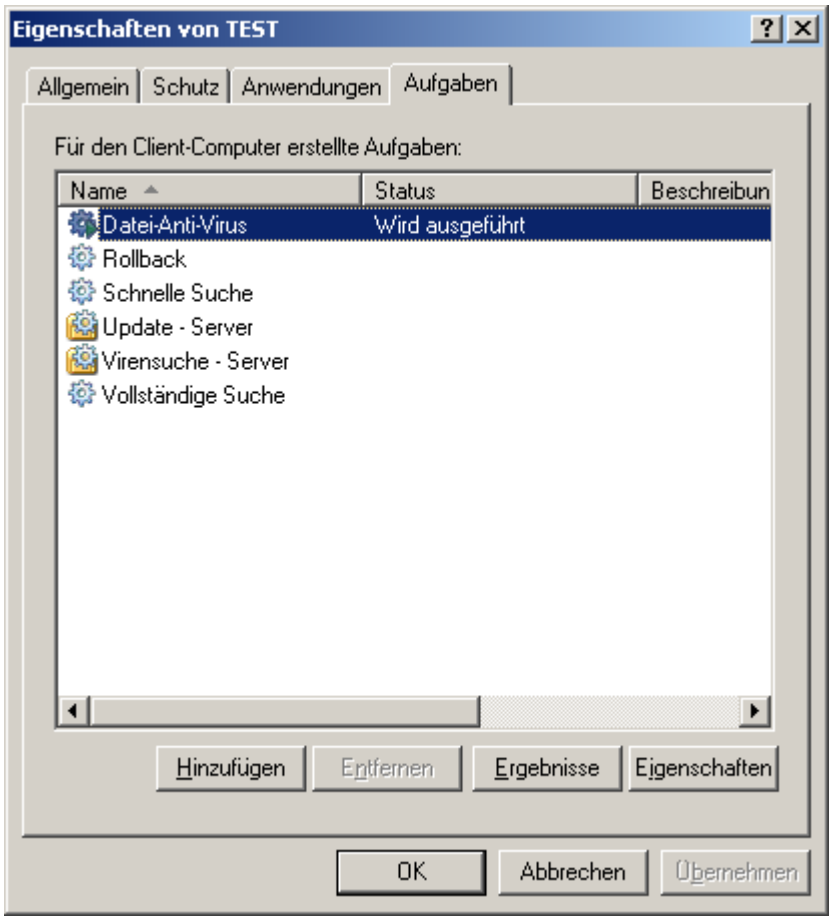


*Abbildung 16. Fenster mit Eigenschaften eines Client-Computers. Registerkarte **Aufgaben***

➧ *Gehen Sie folgendermaßen vor, um eine Liste der für einen Client-Computer erstellten Aufgaben anzuzeigen:*

1. Öffnen Sie die Administrationskonsole von KasperskyAdministration Kit.
2. Öffnen Sie im Ordner **Verwaltete Computer** den Ordner der Gruppe, zu der der Client-Computer gehört.
3. Öffnen Sie in der gewählten Gruppe den Unterordner **Client-Computer** und wählen Sie im Detailfenster einen Computer aus, für den die Anwendungsparameter geändert werden sollen.
4. Verwenden Sie im Kontextmenü den Befehl **Eigenschaften** oder den entsprechenden Punkt im Menü **Aktion**, um das Eigenschaftenfenster des Client-Computers zu öffnen.

5. Öffnen Sie im folgenden Eigenschaftenfenster des Client-Computers die Registerkarte **Aufgaben**. Sie enthält eine vollständige Liste der für diesen Client-Computer erstellten Aufgaben.

AUFGABEN STARTEN UND BEENDEN

Aufgaben werden nur dann auf einem Computer ausgeführt, wenn die entsprechende Anwendung gestartet wurde (s. S. 124). Beim Beenden der Anwendung werden laufende Aufgaben abgebrochen.

Der Start und das Beenden von Aufgaben erfolgt automatisch (entsprechend einem Zeitplan) oder manuell (mit Hilfe der Befehle des Kontextmenüs) sowie aus dem Eigenschaftenfenster einer Aufgabe. Sie können den Ausführungsprozess einer laufenden Aufgabe anhalten und fortsetzen.

Gehen Sie folgendermaßen vor, um eine Aufgabe manuell zu starten, zu beenden, anzuhalten oder fortzusetzen:

1. Öffnen Sie das Eigenschaftenfenster des Client-Computers auf der Registerkarte **Aufgaben**.

2. Markieren Sie die gewünschte Aufgabe und öffnen Sie ihr Kontextmenü. Wählen Sie den Punkt **Starten**, um die Aufgabe zu starten, oder den Punkt **Beenden**, um sie zu beenden. Es können auch die entsprechenden Punkte im Menü **Aktion** verwendet werden.

   Eine Aufgabe kann nicht aus dem Kontextmenü angehalten oder fortgesetzt werden.

   oder

   Markieren Sie die gewünschte Aufgabe in der Liste und klicken Sie auf die Schaltfläche **Eigenschaften**. Im folgenden Eigenschaftenfenster können Sie die Aufgabe auf der Registerkarte **Allgemein** mit Hilfe der entsprechenden Schaltflächen starten, beenden, anhalten oder fortsetzen.

AUFGABE ERSTELLEN

Bei der Arbeit mit Kaspersky Anti-Virus über Kaspersky Administration Kit können Sie folgende Aufgabentypen erstellen:

- lokale Aufgaben, die für einen einzelnen Client-Computer erstellt werden.
- Gruppenaufgaben, die für Client-Computer erstellt werden, die einer Verwaltungsgruppe angehören.
- Aufgaben für eine Auswahl von Computern, die für Computer außerhalb von Verwaltungsgruppen erstellt werden.
- Aufgaben für Kaspersky Administration Kit – spezifische Aufgaben für den Updateserver: Aufgaben zum Download von Updates, Aufgaben zum Anlegen von Sicherungskopien und Aufgaben zum Senden von Berichten.

  Aufgaben für eine Auswahl von Computern werden nur für die festgelegte Auswahl von Computern ausgeführt. Wenn zu einer Gruppe, für deren Computer eine Remote-Installationsaufgabe erstellt wurde, neue Client-Computer hinzugefügt werden, dann wird diese Aufgabe für die neuen Computer nicht ausgeführt. In diesem Fall muss eine neue Aufgabe erstellt oder die Einstellungen der vorhandenen Aufgabe müssen entsprechend angepasst werden.

Es können folgende Aktionen mit Aufgaben ausgeführt werden:

- Aufgabenparameter anpassen.
- Aufgabenausführung überwachen.

- Aufgabe aus einer Gruppe in eine andere kopieren und verschieben, Aufgabe löschen. Dazu dienen die Standardbefehle des Kontextmenüs **Kopieren / Einfügen, Ausschneiden/ Einfügen und Löschen** bzw. die entsprechenden Punkte im Menü **Aktion**.

- Aufgaben importieren und exportieren.

Nähere Informationen über die Arbeit mit Aufgaben finden Sie im Handbuch zu Kaspersky Administration Kit.

Gehen Sie folgendermaßen vor, um eine lokale Aufgabe zu erstellen:

1. Ö ffnen Sie das Eigenschaftenfenster des entsprechenden Client-Computers auf der Registerkarte **Aufgaben**.
2. Klicken Sie auf die Schaltfläche **Hinzufügen**.
3. Dadurch wird der Assistent für neue Aufgaben gestartet (auf S. 130). Folgen Sie den Anweisungen.

Gehen Sie folgendermaßen vor, um eine Gruppenaufgabe zu erstellen:

1. Öffnen Sie die Administrationskonsole von Kaspersky Administration Kit.
2. Öffnen Sie im Ordner **Verwaltete Computer** den Ordner der entsprechenden Gruppe.
3. Öffnen Sie in der gewählten Gruppe den Unterordner **Gruppenaufgaben**, der alle für diese Gruppe erstellten Aufgaben enthält.
4. Starten Sie im Aufgabenbereich mit dem Link **Neue Aufgabe erstellen** den Assistenten für neue Aufgaben. Informationen über Besonderheiten beim Erstellen von Gruppenaufgaben finden Sie im Handbuch zu Kaspersky Administration Kit.

Gehen Sie folgendermaßen vor, um eine Aufgabe für eine Auswahl von Computern (eine Aufgabe für Kaspersky Administration Kit) zu erstellen:

1. Öffnen Sie die Administrationskonsole von Kaspersky Administration Kit.
2. Wählen Sie den Ordner **Aufgaben für Zusammenstellung von Computern** (**Aufgaben von Kaspersky Administration Kit**).
3. Starten Sie im Aufgabenbereich mit dem Link **Neue Aufgabe erstellen** den Assistenten für neue Aufgaben. Informationen über Besonderheiten beim Erstellen von Aufgaben für Kaspersky Administration Kit für eine Auswahl von Computern finden Sie im Handbuch zu Kaspersky Administration Kit.

ASSISTENT FÜR NEUE LOKALE AUFGABEN

Der Assistent für neue lokale Aufgaben wird durch Auswahl des entsprechenden Befehls im Kontextmenü eines Client-Computers oder in dessen Eigenschaftenfenster gestartet.

Der Assistent besteht aus einer Reihe von Fenstern (Schritten). Zur Navigation zwischen den Fenstern dienen die Schaltflächen **Zurück** und **Weiter**, zum Abschluss des Assistenten die Schaltfläche **Fertig**. Die Arbeit des Assistenten kann auf einer beliebigen Etappe durch Klick auf die Schaltfläche **Abbrechen** beendet werden.

SCHRITT 1. ALLGEMEINE ANGABEN ÜBER DIE AUFGABE EINGEBEN

Das erste Fenster des Assistenten dient der Eingabe des Aufgabennamens (Feld **Name**).

SCHRITT 2. ANWENDUNG UND AUFGABENTYP WÄHLEN

Auf dieser Etappe wird die Anwendung angegeben, für die eine Aufgabe erstellt werden soll – Kaspersky Anti-Virus 6.0 für Windows Server MP4 oder Administrationsagent. Außerdem muss ein Aufgabentyp ausgewählt werden. Für Kaspersky Anti-Virus 6.0 können folgende Aufgaben erstellt werden:

- *Virensuche* – Aufgabe zur Virensuche in benutzerdefinierten Bereichen.
- *Update* – Aufgabe zum Download und zum Übernehmen eines Updatepakets für die Anwendung.
- *Rollback des Updates* – Aufgabe zum Rollback des letzten Updates der Anwendung.
- *Schlüsseldatei installieren* – Aufgabe zur Installation einer Schlüsseldatei für eine neue Lizenz, die für die Arbeit der Anwendung erforderlich ist.

SCHRITT 3. PARAMETER DES GEWÄHLTEN AUFGABENTYPS ANPASSEN

Abhängig vom Aufgabentyp, der beim vorherigen Schritt ausgewählt wurde, variiert der Inhalt des Konfigurationsfensters.

Für die Aufgabe zur Virensuche muss die Aktion angegeben werden (auf S. 53), die Kaspersky Anti-Virus beim Fund eines gefährlichen Objekts ausführen soll. Außerdem wird hier eine Liste der Untersuchungsobjekte angelegt (auf S. 52).

Für die Aufgabe zum Update der Datenbanken und Module der Anwendung ist die Angabe der Quelle erforderlich, von der die Updates heruntergeladen werden sollen (s. S. 65). In der Grundeinstellung erfolgt das Update vom Updateserver der Anwendung Kaspersky Administration Kit.

Die Aufgabe Rollback des Updates besitzt keine spezifischen Einstellungen.

Für die Aufgabe zur Installation einer Schlüsseldatei wird mit Hilfe der Schaltfläche **Durchsuchen** der Pfad einer Schlüsseldatei angegeben. Um eine Datei als Schlüsseldatei für eine Reservelizenz hinzuzufügen, aktivieren Sie das entsprechende Kontrollkästchen ☑. Die Reservelizenz wird aktiviert, wenn die Gültigkeitsdauer der aktiven Lizenz abläuft.

Informationen über eine bestimmte Lizenz (Nummer, Typ und Gültigkeit der Lizenz) werden im Feld unten angezeigt.

SCHRITT 4. ZEITPLAN ANPASSEN

Nachdem Sie die Aufgabenparameter angepasst haben, wird Ihnen angeboten, den Zeitplan für den automatischen Aufgabenstart anzupassen.

Wählen Sie dazu im Fenster mit den Zeitplaneinstellungen aus der Dropdown-Liste eine Frequenz für den Aufgabenstart aus und stellen Sie im unteren Teil die Details ein.

SCHRITT 5. ERSTELLEN DER AUFGABE ABSCHLIEßEN

Im letzten Fenster des Assistenten werden Sie über den erfolgreichen Abschluss des Vorgangs zum Erstellen der Aufgabe informiert.

AUFGABENPARAMETER ANPASSEN

Die Konfiguration von Aufgabenparametern der Anwendung über das Interface von Kaspersky Administration Kit entspricht der Konfiguration über das lokale Interface von Kaspersky Anti-Virus. Eine Ausnahme bilden die für Kaspersky Administration Kit spezifischen Parameter (z.B. Parameter, die einem Benutzer die Verwaltung lokaler Untersuchungsaufgaben erlauben oder verbieten).

Wenn für eine Anwendung eine Richtlinie erstellt wurde (s. S. 134), durch die das Ändern bestimmter Parameter verboten wird, dann können diese beim Anpassen der Aufgabenparameter nicht geändert werden.

Alle Registerkarten im Eigenschaftenfenster einer Aufgabe unter Ausnahme der Registerkarte **Einstellungen** (s. Abb. unten) sind für die Anwendung Kaspersky Administration Kit standardmäßig und werden im entsprechenden Handbuch ausführlich beschrieben. Die Registerkarte **Einstellungen** enthält spezifische Parameter für Kaspersky Anti-Virus. Der Inhalt variiert in Abhängigkeit vom ausgewählten Aufgabentyp.

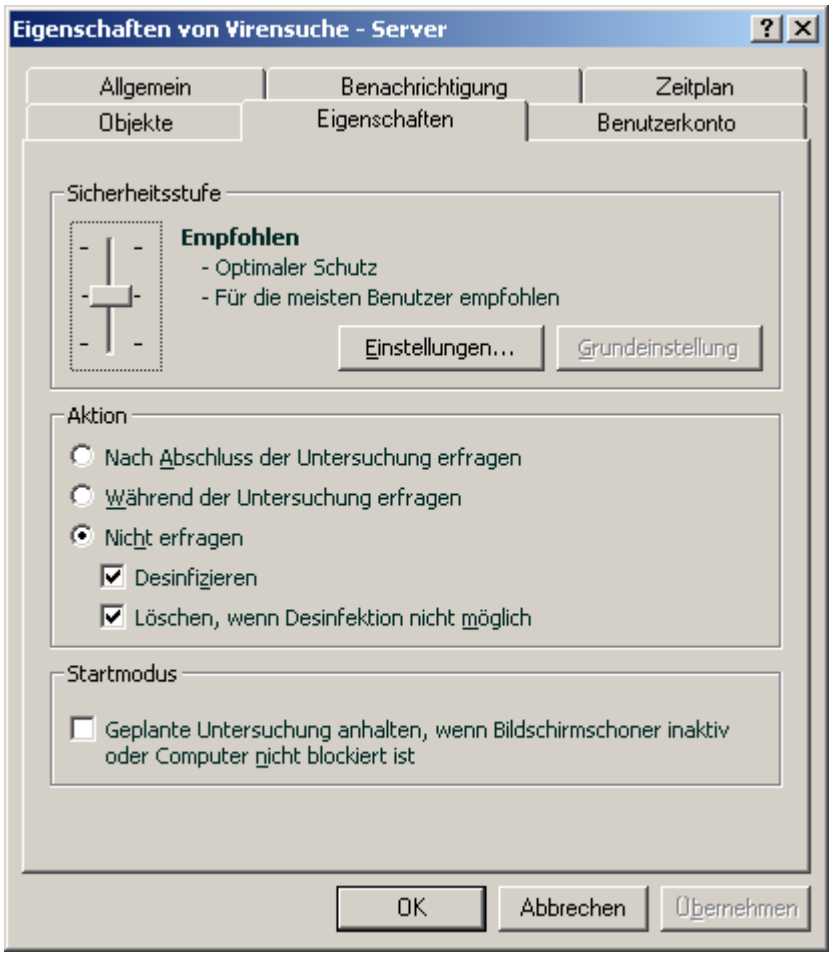


*Abbildung 17. Eigenschaftenfenster einer Aufgabe. Registerkarte **Einstellungen***

Gehen Sie folgendermaßen vor, um eine lokale Aufgabe anzuzeigen und anzupassen:

1. Öffnen Sie das Eigenschaftenfenster des Client-Computers auf der Registerkarte **Aufgaben**.
2. Markieren Sie die Liste in der Liste und verwenden Sie die Schaltfläche **Eigenschaften**. Dadurch wird das Konfigurationsfenster für die Anwendungsparameter geöffnet.

Gehen Sie folgendermaßen vor, um zu den Gruppenaufgaben zu wechseln:

1. Öffnen Sie die Administrationskonsole von Kaspersky Administration Kit.
2. Öffnen Sie im Ordner **Verwaltete Computer** den Ordner der entsprechenden Gruppe.
3. Öffnen Sie in der gewählten Gruppe den Unterordner **Gruppenaufgaben**, der alle für diese Gruppe erstellten Aufgaben enthält.
4. Markieren Sie in der Konsolenstruktur die gewünschte Aufgabe, um ihre Eigenschaften anzuzeigen und anzupassen.

   Der Aufgabenbereich enthält zusammenfassende Informationen über die Aufgabe und bietet Links zur Ausführung der Ausgabe und zum Anpassen der Aufgabenparameter. Informationen über Besonderheiten von Gruppenaufgaben finden Sie im Handbuch zu Kaspersky Administration Kit.

Gehen Sie folgendermaßen vor, um zu den Aufgaben für die Zusammenstellungen von Computern (Aufgaben für Kaspersky Administration Kit) zu wechseln:

1. Öffnen Sie die Administrationskonsole von Kaspersky Administration Kit.
2. Wählen Sie den Ordner **Aufgaben für Zusammenstellung von Computern** (**Aufgaben von Kaspersky Administration Kit**).
3. Markieren Sie in der Konsolenstruktur die gewünschte Aufgabe, um ihre Eigenschaften anzuzeigen und anzupassen.

   Der Aufgabenbereich enthält zusammenfassende Informationen über die Aufgabe und bietet Links zur Ausführung der Ausgabe und zum Anpassen der Aufgabenparameter. Informationen über Besonderheiten beim Erstellen von Aufgaben für Kaspersky Administration Kit für die Zusammenstellungen von Computern finden Sie im Handbuch zu Kaspersky Administration Kit.

VERWALTUNG VON RICHTLINIEN

Das Festlegen von Richtlinien erlaubt es, einheitliche Anwendungs- und Aufgabeneinstellungen auf die Client-Computer zu verteilen, die zu einer Verwaltungsgruppe gehören.

Dieser Abschnitt enthält Informationen über das Erstellen und die Konfiguration einer Richtlinie für Kaspersky Anti-Virus 6.0 für Windows Server MP4. Nähere Informationen zur Konzeption der Richtlinienverwaltung über Kaspersky Administration Kit finden Sie im entsprechenden Administratorhandbuch.

Sie können ein vollständiges oder teilweises Verbot für das Ändern von Parametern einer Richtlinie festlegen, das sich auf Richtlinien untergeordneter Gruppen, Aufgabenparameter und Anwendungsparameter bezieht. Klicken Sie dazu auf die Schaltfläche  . Für Parameter, deren Änderung verboten ist, besitzt die Schaltfläche folgendes Aussehen:  .

Gehen Sie folgendermaßen vor, um eine Liste der für Kaspersky Anti-Virus erstellten Richtlinien zu öffnen:

1. Öffnen Sie die Administrationskonsole von Kaspersky Administration Kit.
2. Öffnen Sie im Ordner **Verwaltete Computer** den Ordner der Gruppe, zu der der Client-Computer gehört.
3. Öffnen Sie in der gewählten Gruppe den Unterordner **Richtlinien**, in der Konsolenstruktur werden alle für diese Gruppe erstellten Richtlinien angezeigt.

RICHTLINIE ERSTELLEN

Wenn Kaspersky Anti-Virus über Kaspersky Administration Kit verwaltet wird, können Sie entsprechende Richtlinien festlegen.

Es können folgende Aktionen mit Richtlinien ausgeführt werden:

- Parameter einer Richtlinie anpassen.
- Aufgabe aus einer Gruppe in eine andere kopieren und verschieben, Aufgabe löschen. Dazu dienen die Standardbefehle des Kontextmenüs **Kopieren / Einfügen, Ausschneiden/ Einfügen und Löschen** bzw. die entsprechenden Punkte im Menü **Aktion**.
- Richtlinie importieren und exportieren.

Nähere Informationen über die Arbeit mit Richtlinien finden Sie im Handbuch zu Kaspersky Administration Kit.

Gehen Sie folgendermaßen vor, um eine Richtlinie zu erstellen:

1. Öffnen Sie die Administrationskonsole von Kaspersky Administration Kit.

2. Öffnen Sie im Ordner **Verwaltete Computer** den Ordner der entsprechenden Gruppe.

3. Öffnen Sie in der gewählten Gruppe den Unterordner **Richtlinien**, der alle für diese Gruppe erstellten Richtlinien enthält.

4. Starten Sie im Aufgabenbereich mit dem Link **Neue Richtlinie erstellen** den Assistenten für neue Aufgaben.

5. Im folgenden Fenster wird der Assistent für neue Richtlinien gestartet (s. S. 134), Folgen Sie den Anweisungen.

ASSISTENT FÜR NEUE RICHTLINIEN

Der Assistent für neue Richtlinien wird durch Auswahl des entsprechenden Befehls im Kontextmenü des Ordners **Richtlinien** der entsprechenden Verwaltungsgruppe oder des Links im Detailfenster (für den Ordner **Richtlinien**) gestartet.

Der Assistent besteht aus einer Reihe von Fenstern (Schritten). Zur Navigation zwischen den Fenstern dienen die Schaltflächen **Zurück** und **Weiter**, zum Abschluss des Assistenten die Schaltfläche **Fertig**. Die Arbeit des Assistenten kann auf einer beliebigen Etappe durch Klick auf die Schaltfläche **Abbrechen** beendet werden.

SCHRITT 1. ALLGEMEINE ANGABEN ÜBER DIE RICHTLINIE EINGEBEN

Das erste Fenster des Assistenten dient der Eingabe. Hier wird ein Name für die Richtlinie eingegeben (Feld **Name**) und die Anwendung **Kaspersky Anti-Virus 6.0 für Windows Server MP4** wird aus der Dropdown-Liste **Anwendungsname** ausgewählt.

Wenn der Assistent für neue Richtlinien aus dem Aufgabenbereich des Knotens **Richtlinien** gestartet wurde (mit dem Link **Richtlinie erstellen für Kaspersky Anti-Virus für Windows Server MP4**), dann fehlt die Auswahl der Anwendung.

Wenn Sie eine Richtlinie auf der Basis einer vorhandenen Richtlinie für eine vorherige Programmversion erstellen möchten, aktivieren Sie das Kontrollkästchen ☑ **Parameter aus einer vorhandenen Richtlinie übernehmen** und wählen Sie eine Richtlinie aus, deren Parameter in einer neuen Richtlinie verwendet werden. Um eine Richtlinie zu bestimmen, klicken Sie auf die Schaltfläche **Auswählen**. Dadurch wird eine Liste mit vorhandenen Richtlinien geöffnet, die beim Erstellen einer Richtlinie verwendet werden können.

SCHRITT 2. STATUS DER RICHTLINIE WÄHLEN

In diesem Fenster wird der Status festgelegt, den die Richtlinie nach dem Erstellen besitzen soll. Wählen Sie eine Variante aus: aktive Richtlinie, inaktive Richtlinie. Nähere Informationen über die Status von Richtlinien finden Sie im Handbuch zu Kaspersky Administration Kit.

In einer Gruppe können mehrere Richtlinien für eine Anwendung erstellt werden. Allerdings kann nur eine davon als aktive Richtlinie gelten.

SCHRITT 3. IMPORT VON PROGRAMMPARAMETERN

Wenn Sie über eine früher gespeicherte Konfigurationsdatei für die Anwendung verfügen, können Sie die Datei bei diesem Schritt mit der Schaltfläche **Laden** angegeben. In diesem Fall werden in den folgenden Fenstern des Assistenten die importierten Parameter angezeigt.

SCHRITT 4. EINSTELLUNG DER SCHUTZPARAMETER

Auf dieser Etappe können Sie die Schutzkomponenten, die in einer Richtlinie verwendet werden, aktivieren (deaktivieren) und anpassen.

Standardmäßig sind alle Schutzkomponenten aktiviert. Um eine der Komponenten zu deaktivieren, entfernen Sie das entsprechende Kontrollkästchen. Um eine Schutzkomponente im Detail anzupassen, wählen Sie die Komponente in der Liste aus und klicken Sie auf die Schaltfläche **Einstellungen**.

SCHRITT 5. ANPASSEN DES KENNWORTSCHUTZES

In diesem Fenster des Assistenten können Sie den Kennwortschutz für die Arbeit mit dem Programm und seine Deinstallation anpassen.

SCHRITT 6. ANPASSEN DER VERTRAUENSWÜRDIGEN ZONE

In diesem Fenster des Assistenten kann die vertrauenswürdige Zone angepassst werden: Sie können der Liste für vertrauenswürdige Anwendungen Programme hinzufügen, die zur Netzwerkverwaltung dienen, und bestimmte Dateitypen aus dem Untersuchungsbereich ausschließen.

SCHRITT 7. EINSTELLUNGEN FÜR DIE INTERAKTION MIT DEM BENUTZER

Bei diesem Schritt können Sie die Parameter für die Interaktion zwischen Benutzer und Kaspersky Anti-Virus festlegen:

- Anzeigen der Programmoberfläche auf einem Remote-Computer.
- Benachrichtigung des Benutzers über Ereignisse.
- Anzeige und Animation des Programmsymbols im Meldungsbereich der Taskleiste.
- "Protected by Kaspersky Lab" über dem Microsoft Windows-Begrüßungsbildschirm anzeigen.
- Anzeige des Programms im Startmenü.
- Anzeige in der Liste der installierten Programme.

SCHRITT 8. ERSTELLEN DER RICHTLINIE ABSCHLIEßEN

Im letzten Fenster des Assistenten werden Sie darüber informiert, dass der Vorgang zum Erstellen der Richtlinie erfolgreich abgeschlossen wurde.

Nachdem die Arbeit des Assistenten wird die Richtlinie für die angegebene Anwendung dem Ordner **Richtlinien** der entsprechenden Verwaltungsgruppe hinzugefügt und in der Konsolenstruktur angezeigt.

Die Parameter einer Richtlinie können angepasst werden und mit Hilfe der Schaltflächen  und  kann das Ändern der einzelnen Parametergruppen eingeschränkt werden. Das Symbol  bedeutet, dass der Benutzer auf dem Client-Computer die Einstellungen nicht ändern kann. Das Symbol  bedeutet, dass der Benutzer Zugriff auf die Parameter besitzt. Die Verteilung einer Richtlinie an die Client-Computer erfolgt bei der ersten Synchronisierung der Clients mit dem Server.

PARAMETER EINER RICHTLINIE ANPASSEN

Auf dieser Etappe können Sie in der Richtlinie Änderungen vornehmen und ein Verbot für das Ändern von Parametern in den Richtlinien untergeordneter Gruppen, in den Anwendungsparametern und Aufgabenparametern festlegen. Die Parameter einer Richtlinie werden im Eigenschaftenfenster der Richtlinie angepasst (s. Abb. unten).

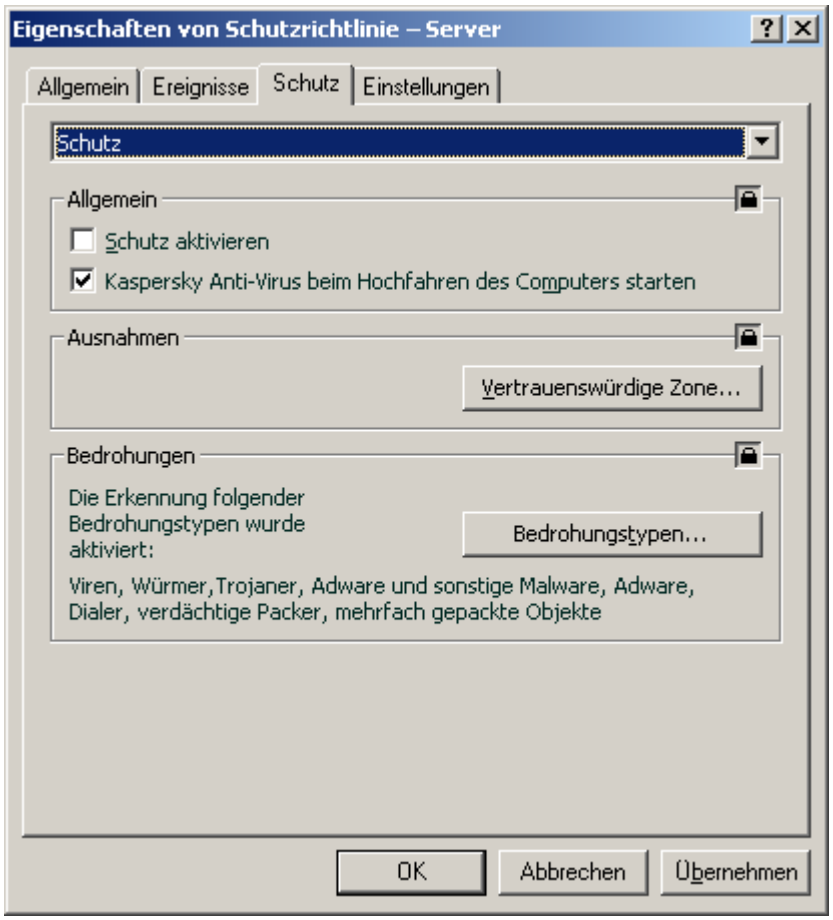


*Abbildung 18. Eigenschaftenfenster einer Richtlinie. Registerkarte **Schutz***

Alle Registerkarten (unter Ausnahme der Registerkarten **Schutz** und **Einstellungen**) sind für die Anwendung Kaspersky Administration Kit standardmäßig. Sie werden im entsprechenden Handbuch ausführlich beschrieben.

Die Parameter einer Richtlinie für Kaspersky Anti-Virus 6.0 umfassen Anwendungsparameter (s. S. 125) und Aufgabenparameter. Die Registerkarte **Einstellungen** enthält die Anwendungsparameter, die Registerkarte **Schutz** die Aufgabenparameter.

Um die Parameter anzupassen, wählen Sie aus der Dropdown-Liste im oberen Bereich des Fensters den erforderlichen Wert aus und nehmen Sie die Einstellungen vor.

➡ *Gehen Sie folgendermaßen vor, um die Parameter einer Richtlinie anzuzeigen und anzupassen:*

1. Öffnen Sie die Administrationskonsole von Kaspersky Administration Kit.
2. Öffnen Sie im Ordner **Verwaltete Computer** den Ordner der entsprechenden Gruppe.
3. Öffnen Sie in der gewählten Gruppe den Unterordner **Richtlinien**, der alle für diese Gruppe erstellten Richtlinien enthält.
4. Markieren Sie in der Konsolenstruktur die gewünschte Richtlinie, um ihre Eigenschaften anzuzeigen und anzupassen.

5. Der Aufgabenbereich enthält zusammenfassende Informationen über die Richtlinie und bietet Links zur Verwaltung des Richtlinienstatus und zum Anpassen der Richtlinienparameter.

   oder

   Öffnen Sie das Kontextmenü der ausgewählten Richtlinie und öffnen Sie mit dem Punkt **Eigenschaften** das Konfigurationsfenster der Richtlinie für Kaspersky Anti-Virus.

   Informationen über Besonderheiten bei der Arbeit mit Richtlinien finden Sie im Handbuch zu Kaspersky Administration Kit.

VERWENDUNG DES CODES VON DRITTHERSTELLERN

Bei der Entwicklung von Kaspersky Anti-Virus wurde der Code von Drittherstellern verwendet.

IN DIESEM ABSCHNITT

BIBLIOTHEK BOOST-1.30.0

Bei der Entwicklung des Programms wurde die Bibliothek Boost-1.30.0 verwendet.

Boost Software License - Version 1.0 - August 17th, 2003

Permission is hereby granted, free of charge, to any person or organization obtaining a copy of the software and accompanying documentation covered by this license (the "Software") to use, reproduce, display, distribute, execute, and transmit the Software, and to prepare derivative works of the

Software, and to permit third-parties to whom the Software is furnished to do so, all subject to the following:

The copyright notices in the Software and this entire statement, including the above license grant, this restriction and the following disclaimer, must be included in all copies of the Software, in whole or in part, and all derivative works of the Software, unless such copies or derivative works are solely in the form of machine-executable object code generated by a source language processor.

THE SOFTWARE IS PROVIDED "AS IS", WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO THE WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, TITLE AND NON-INFRINGEMENT. IN NO EVENT SHALL THE COPYRIGHT HOLDERS OR ANYONE DISTRIBUTING THE SOFTWARE BE LIABLE FOR ANY DAMAGES OR OTHER LIABILITY, WHETHER IN CONTRACT, TORT OR OTHERWISE, ARISING FROM, OUT OF OR IN CONNECTION WITH THE SOFTWARE OR THE USE OR OTHER DEALINGS IN THE SOFTWARE.

BIBLIOTHEK LZMA SDK 4.40, 4.43

Bei der Entwicklung des Programms wurde die Bibliothek Bibliothek LZMA SDK 4.40, 4.43 verwendet.

BIBLIOTHEK WINDOWS TEMPLATE LIBRARY 7.5

Bei der Entwicklung des Programms wurde die Bibliothek Windows Template Library 7.5 verwendet.

Copyright (C) 2006, Microsoft Corporation

Microsoft Public License (Ms-PL)

Published: October 12, 2006

This license governs use of the accompanying software. If you use the software, you accept this license. If you do not accept the license, do not use the software.

1. Definitions

The terms "reproduce", "reproduction", "derivative works", and "distribution" have the same meaning here as under U.S. copyright law.

A "contribution" is the original software, or any additions or changes to the software.

A "contributor" is any person that distributes its contribution under this license.

"Licensed patents" are a contributor’s patent claims that read directly on its contribution.

2. Grant of Rights

(A) Copyright Grant- Subject to the terms of this license, including the license conditions and limitations in section 3, each contributor grants you a non-exclusive, worldwide, royalty-free copyright license to reproduce its contribution, prepare derivative works of its contribution, and distribute its contribution or any derivative works that you create.

(B) Patent Grant- Subject to the terms of this license, including the license conditions and limitations in section 3, each contributor grants you a non-exclusive, worldwide, royalty-free license under its licensed patents to make, have made, use, sell, offer for sale, import, and/or otherwise dispose of its contribution in the software or derivative works of the contribution in the software.

3. Conditions and Limitations

(A) No Trademark License- This license does not grant you rights to use any contributors' name, logo, or trademarks.

(B) If you bring a patent claim against any contributor over patents that you claim are infringed by the software, your patent license from such contributor to the software ends automatically.

(C) If you distribute any portion of the software, you must retain all copyright, patent, trademark, and attribution notices that are present in the software.

(D) If you distribute any portion of the software in source code form, you may do so only under this license by including a complete copy of this license with your distribution. If you distribute any portion of the software in compiled or object code form, you may only do so under a license that complies with this license.

(E) The software is licensed "as-is." You bear the risk of using it. The contributors give no express warranties, guarantees or conditions. You may have additional consumer rights under your local laws which this license cannot change. To the extent permitted under your local laws, the contributors exclude the implied warranties of merchantability, fitness for a particular purpose and non-infringement.

BIBLIOTHEK WINDOWS INSTALLER XML (WIX) TOOLSET 2.0

Bei der Entwicklung des Programms wurde die Bibliothek Windows Installer XML (WiX) toolset 2.0 verwendet.

Copyright (C) 2009, Microsoft Corporation

Common Public License Version 1,0

THE ACCOMPANYING PROGRAM IS PROVIDED UNDER THE TERMS OF THIS COMMON PUBLIC LICENSE ("AGREEMENT"). ANY USE, REPRODUCTION OR DISTRIBUTION OF THE PROGRAM CONSTITUTES RECIPIENT'S ACCEPTANCE OF THIS AGREEMENT.

1. DEFINITIONS

"Contribution" means:

a) in the case of the initial Contributor, the initial code and documentation distributed under this Agreement, and

b) in the case of each subsequent Contributor:

i) changes to the Program, and

ii) additions to the Program;

where such changes and/or additions to the Program originate from and are distributed by that particular Contributor. A Contribution 'originates' from a Contributor if it was added to the Program by such Contributor itself or anyone acting on such Contributor's behalf. Contributions do not include additions to the Program which: (i) are separate modules of software distributed in conjunction with the Program under their own license agreement, and (ii) are not derivative works of the Program.

"Contributor" means any person or entity that distributes the Program.

"Licensed Patents" mean patent claims licensable by a Contributor which are necessarily infringed by the use or sale of its Contribution alone or when combined with the Program.

"Program" means the Contributions distributed in accordance with this Agreement.

"Recipient" means anyone who receives the Program under this Agreement, including all Contributors.

2. GRANT OF RIGHTS

a) Subject to the terms of this Agreement, each Contributor hereby grants Recipient a non-exclusive, worldwide, royalty-free copyright license to reproduce, prepare derivative works of, publicly display, publicly perform, distribute and sublicense the Contribution of such Contributor, if any, and such derivative works, in source code and object code form.

b) Subject to the terms of this Agreement, each Contributor hereby grants Recipient a non-exclusive, worldwide, royalty-free patent license under Licensed Patents to make, use, sell, offer to sell, import and otherwise transfer the Contribution of such Contributor, if any, in source code and object code form. This patent license shall apply to the combination of the Contribution and the Program if, at the time the Contribution is added by the Contributor, such addition of the Contribution causes such combination to be covered by the Licensed Patents. The patent license shall not apply to any other combinations which include the Contribution. No hardware per se is licensed hereunder.

c) Recipient understands that although each Contributor grants the licenses to its Contributions set forth herein, no assurances are provided by any Contributor that the Program does not infringe the patent or other intellectual property rights of any other entity. Each Contributor disclaims any liability to Recipient for claims brought by any other entity based on infringement of intellectual property rights or otherwise. As a condition to exercising the rights and licenses granted hereunder, each Recipient hereby assumes sole responsibility to secure any other intellectual property rights needed, if any. For example, if a third party patent license is required to allow Recipient to distribute the Program, it is Recipient's responsibility to acquire that license before distributing the Program.

d) Each Contributor represents that to its knowledge it has sufficient copyright rights in its Contribution, if any, to grant the copyright license set forth in this Agreement.

3. REQUIREMENTS

A Contributor may choose to distribute the Program in object code form under its own license agreement, provided that:

a) it complies with the terms and conditions of this Agreement; and

b) its license agreement:

i) effectively disclaims on behalf of all Contributors all warranties and conditions, express and implied, including warranties or conditions of title and non-infringement, and implied warranties or conditions of merchantability and fitness for a particular purpose;

ii) effectively excludes on behalf of all Contributors all liability for damages, including direct, indirect, special, incidental and consequential damages, such as lost profits;

iii) states that any provisions which differ from this Agreement are offered by that Contributor alone and not by any other party; and

iv) states that source code for the Program is available from such Contributor, and informs licensees how to obtain it in a reasonable manner on or through a medium customarily used for software exchange.

When the Program is made available in source code form:

a) it must be made available under this Agreement; and

b) a copy of this Agreement must be included with each copy of the Program.

Contributors may not remove or alter any copyright notices contained within the Program.

Each Contributor must identify itself as the originator of its Contribution, if any, in a manner that reasonably allows subsequent Recipients to identify the originator of the Contribution.

4. COMMERCIAL DISTRIBUTION

Commercial distributors of software may accept certain responsibilities with respect to end users, business partners and the like. While this license is intended to facilitate the commercial use of the Program, the Contributor who includes the Program in a commercial product offering should do so in a manner which does not create potential liability for other Contributors. Therefore, if a Contributor includes the Program in a commercial product offering, such Contributor ("Commercial Contributor") hereby agrees to defend and indemnify every other Contributor ("Indemnified Contributor") against any losses, damages and costs (collectively "Losses") arising from claims, lawsuits and other legal actions brought by a third party against the Indemnified Contributor to the extent caused by the acts or omissions of such Commercial Contributor in connection with its distribution of the Program in a commercial product offering. The obligations in this section do not apply to any claims or Losses relating to any actual or alleged intellectual property infringement. In order to qualify, an Indemnified Contributor must: a) promptly notify the Commercial Contributor in writing of such claim, and b) allow the Commercial Contributor to control, and cooperate with the Commercial Contributor in, the defense and any related settlement negotiations. The Indemnified Contributor may participate in any such claim at its own expense.

For example, a Contributor might include the Program in a commercial product offering, Product X. That Contributor is then a Commercial Contributor. If that Commercial Contributor then makes performance claims, or offers warranties related to Product X, those performance claims and warranties are such Commercial Contributor's responsibility alone. Under this section, the Commercial Contributor would have to defend claims against the other Contributors related to those performance claims and warranties, and if a court requires any other Contributor to pay any damages as a result, the Commercial Contributor must pay those damages.

5. NO WARRANTY

EXCEPT AS EXPRESSLY SET FORTH IN THIS AGREEMENT, THE PROGRAM IS PROVIDED ON AN "AS IS" BASIS, WITHOUT WARRANTIES OR CONDITIONS OF ANY KIND, EITHER EXPRESS OR IMPLIED INCLUDING, WITHOUT LIMITATION, ANY WARRANTIES OR CONDITIONS OF TITLE, NON-INFRINGEMENT, MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE. Each Recipient is solely responsible for determining the appropriateness of using and distributing the Program and assumes all risks associated with its exercise of rights under this Agreement, including but not limited to the risks and costs of program errors, compliance with applicable laws, damage to or loss of data, programs or equipment, and unavailability or interruption of operations.

6. DISCLAIMER OF LIABILITY

EXCEPT AS EXPRESSLY SET FORTH IN THIS AGREEMENT, NEITHER RECIPIENT NOR ANY CONTRIBUTORS SHALL HAVE ANY LIABILITY FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING WITHOUT LIMITATION LOST PROFITS), HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OR DISTRIBUTION OF THE PROGRAM OR THE EXERCISE OF ANY RIGHTS GRANTED HEREUNDER, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

7. GENERAL

If any provision of this Agreement is invalid or unenforceable under applicable law, it shall not affect the validity or enforceability of the remainder of the terms of this Agreement, and without further action by the parties hereto, such provision shall be reformed to the minimum extent necessary to make such provision valid and enforceable.

If Recipient institutes patent litigation against a Contributor with respect to a patent applicable to software (including a cross-claim or counterclaim in a lawsuit), then any patent licenses granted by that Contributor to such Recipient under this Agreement shall terminate as of the date such litigation is filed. In addition, if Recipient institutes patent litigation against any entity (including a cross-claim or counterclaim in a lawsuit) alleging that the Program itself (excluding combinations of the Program with other software or hardware) infringes such Recipient's patent(s), then such Recipient's rights granted under Section 2(b) shall terminate as of the date such litigation is filed.

All Recipient's rights under this Agreement shall terminate if it fails to comply with any of the material terms or conditions of this Agreement and does not cure such failure in a reasonable period of time after becoming aware of such noncompliance. If all Recipient's rights under this Agreement terminate, Recipient agrees to cease use and distribution of the Program as soon as reasonably practicable. However, Recipient's obligations under this Agreement and any licenses granted by Recipient relating to the Program shall continue and survive.

Everyone is permitted to copy and distribute copies of this Agreement, but in order to avoid inconsistency the Agreement is copyrighted and may only be modified in the following manner. The Agreement Steward reserves the right to publish new versions (including revisions) of this Agreement from time to time. No one other than the Agreement Steward has the right to modify this Agreement. IBM is the initial Agreement Steward. IBM may assign the responsibility to serve as the Agreement Steward to a suitable separate entity. Each new version of the Agreement will be given a distinguishing version number. The Program (including Contributions) may always be distributed subject to the version of the

Agreement under which it was received. In addition, after a new version of the Agreement is published, Contributor may elect to distribute the Program (including its Contributions) under the new version. Except as expressly stated in Sections 2(a) and 2(b) above, Recipient receives no rights or licenses to the intellectual property of any Contributor under this Agreement, whether expressly, by implication, estoppel or otherwise. All rights in the Program not expressly granted under this Agreement are reserved.

This Agreement is governed by the laws of the State of New York and the intellectual property laws of the United States of America. No party to this Agreement will bring a legal action under this Agreement more than one year after the cause of action arose. Each party waives its rights to a jury trial in any resulting litigation.

BIBLIOTHEK ZIP-2.31

Bei der Entwicklung des Programms wurde die Bibliothek Zip-2.31 verwendet.

Copyright (C) 1990-2005, Info-ZIP

This is version 2005-Feb-10 of the Info-ZIP copyright and license.

The definitive version of this document should be available at

ftp://ftp.info-zip.org/pub/infozip/license.html indefinitely.

Copyright (c) 1990-2005 Info-ZIP. All rights reserved.

For the purposes of this copyright and license, "Info-ZIP" is defined as

the following set of individuals:

Mark Adler, John Bush, Karl Davis, Harald Denker, Jean-Michel Dubois, Jean-loup Gailly, Hunter Goatley, Ed Gordon, Ian Gorman, Chris Herborth, Dirk Haase, Greg Hartwig, Robert Heath, Jonathan Hudson, Paul Kienitz, David Kirschbaum, Johnny Lee, Onno van der Linden, Igor Mandrichenko, Steve P. Miller, Sergio Monesi, Keith Owens, George Petrov, Greg Roelofs, Kai Uwe Rommel, Steve Salisbury, Dave Smith, Steven M. Schweda, Christian Spieler, Cosmin Truta, Antoine Verheijen, Paul von Behren, Rich Wales, Mike White

This software is provided "as is," without warranty of any kind, express or implied. In no event shall Info-ZIP or its contributors be held liable for any direct, indirect, incidental, special or consequential damages arising out of the use of or inability to use this software.

Permission is granted to anyone to use this software for any purpose, including commercial applications, and to alter it and redistribute it freely, subject to the following restrictions:

1. Redistributions of source code must retain the above copyright notice, definition, disclaimer, and this list of conditions.

2. Redistributions in binary form (compiled executables) must reproduce the above copyright notice, definition, disclaimer, and this list of conditions in documentation and/or other materials provided with the distribution. The sole exception to this condition is redistribution of a standard UnZipSFX binary (including SFXWiz) as part of a self-extracting archive; that is permitted without inclusion of this license, as long as the normal SFX banner has not been removed from the binary or disabled.

3. Altered versions--including, but not limited to, ports to new operating systems, existing ports with new graphical interfaces, and dynamic, shared, or static library versions--must be plainly marked as such and must not be misrepresented as being the original source. Such altered versions also must not be misrepresented as being Info-ZIP releases--including, but not limited to, labeling of the altered versions with the names "Info-ZIP" (or any variation thereof, including, but not limited to, different capitalizations), "Pocket UnZip," "WiZ" or "MacZip" without the explicit permission of Info-ZIP. Such altered versions are further prohibited from misrepresentative use of the Zip-Bugs or Info-ZIP e-mail addresses or of the Info-ZIP URL(s).

4. Info-ZIP retains the right to use the names "Info-ZIP," "Zip," "UnZip," "UnZipSFX," "WiZ," "Pocket UnZip," "Pocket Zip," and "MacZip" for its own source and binary releases.

BIBLIOTHEK ZLIB-1.0.4, ZLIB-1.0.8, ZLIB-1.1.3, ZLIB-1.2.3

Bei der Entwicklung des Programms wurde die Bibliothek Zlib-1.0.4, ZLIB-1.0.8, Zlib-1.1.3, Zlib-1.2.3 verwendet.

Copyright (C) 1995-2005, Jean-loup Gailly and Mark Adler

This software is provided 'as-is', without any express or implied warranty. In no event will the authors be held liable for any damages arising from the use of this software.

Permission is granted to anyone to use this software for any purpose, including commercial applications, and to alter it and redistribute it freely, subject to the following restrictions:

1. The origin of this software must not be misrepresented; you must not claim that you wrote the original software. If you use this software in a product, an acknowledgment in the product documentation would be appreciated but is not required.

2. Altered source versions must be plainly marked as such, and must not be misrepresented as being the original software.

3. This notice may not be removed or altered from any source distribution.

Jean-loup Gailly jloup@gzip.org

Mark Adler madler@alumni.caltech.edu

BIBLIOTHEK UNZIP-5.51

Bei der Entwicklung des Programms wurde die Bibliothek UnZip-5.51 verwendet.

Copyright (c) 1990-2004, Info-ZIP

This is version 2004-May-22 of the Info-ZIP copyright and license.

The definitive version of this document should be available at ftp://ftp.info-zip.org/pub/infozip/license.html indefinitely.

Copyright (c) 1990-2004 Info-ZIP. All rights reserved.

For the purposes of this copyright and license, "Info-ZIP" is defined as

the following set of individuals:

Mark Adler, John Bush, Karl Davis, Harald Denker, Jean-Michel Dubois, Jean-loup Gailly, Hunter Goatley, Ian Gorman, Chris Herborth, Dirk Haase, Greg Hartwig, Robert Heath, Jonathan Hudson, Paul Kienitz, David Kirschbaum, Johnny Lee, Onno van der Linden, Igor Mandrichenko, Steve P. Miller, Sergio Monesi, Keith Owens, George Petrov, Greg Roelofs, Kai Uwe Rommel, Steve Salisbury, Dave Smith, Christian Spieler, Antoine Verheijen, Paul von Behren, Rich Wales, Mike White

This software is provided "as is," without warranty of any kind, express or implied. In no event shall Info-ZIP or its contributors be held liable for any direct, indirect, incidental, special or consequential damages arising out of the use of or inability to use this software.

Permission is granted to anyone to use this software for any purpose, including commercial applications, and to alter it and redistribute it freely, subject to the following restrictions:

1. Redistributions of source code must retain the above copyright notice, definition, disclaimer, and this list of conditions.

2. Redistributions in binary form (compiled executables) must reproduce the above copyright notice, definition, disclaimer, and this list of conditions in documentation and/or other materials provided with the distribution. The sole exception to this condition is redistribution of a standard UnZipSFX binary (including SFXWiz) as part of a self-extracting archive; that is permitted without inclusion of this license, as long as the normal SFX banner has not been removed from the binary or disabled.

3. Altered versions--including, but not limited to, ports to new operating systems, existing ports with new graphical interfaces, and dynamic, shared, or static library versions--must be plainly marked as such and must not be misrepresented as being the original source. Such altered versions also must not be misrepresented as being Info-ZIP releases--including, but not limited to, labeling of the altered

versions with the names "Info-ZIP" (or any variation thereof, including, but not limited to, different capitalizations), "Pocket UnZip," "WiZ" or "MacZip" without the explicit permission of Info-ZIP. Such altered versions are further prohibited from misrepresentative use of the Zip-Bugs or Info-ZIP e-mail addresses or of the Info-ZIP URL(s).

4. Info-ZIP retains the right to use the names "Info-ZIP," "Zip," "UnZip," "UnZipSFX," "WiZ," "Pocket UnZip," "Pocket Zip," and "MacZip" for its own source and binary releases.

BIBLIOTHEK LIBPNG-1.0.1, LIBPNG-1.2.8, LIBPNG-1.2.12

Bei der Entwicklung des Programms wurde die Bibliothek libpng-1.0.1, libpng-1.2.8, libpng-1.2.12 verwendet.

This copy of the libpng notices is provided for your convenience. In case of any discrepancy between this copy and the notices in the file png.h that is included in the libpng distribution, the latter shall prevail.

COPYRIGHT NOTICE, DISCLAIMER, and LICENSE:

If you modify libpng you may insert additional notices immediately following

this sentence.

This code is released under the libpng license.

libpng versions 1.2.6, August 15, 2004, through 1.2.39, August 13, 2009, are

Copyright (c) 2004, 2006-2009 Glenn Randers-Pehrson, and are distributed according to the same disclaimer and license as libpng-1.2.5 with the following individual added to the list of Contributing Authors

Cosmin Truta

libpng versions 1.0.7, July 1, 2000, through 1.2.5 - October 3, 2002, are Copyright (c) 2000-2002 Glenn Randers-Pehrson, and are distributed according to the same disclaimer and license as libpng-1.0.6 with the following individuals added to the list of Contributing Authors

Simon-Pierre Cadieux

Eric S. Raymond

Gilles Vollant

and with the following additions to the disclaimer:

There is no warranty against interference with your enjoyment of the library or against infringement. There is no warranty that our efforts or the library will fulfill any of your particular purposes or needs. This library is provided with all faults, and the entire risk of satisfactory quality, performance, accuracy, and effort is with the user.

libpng versions 0.97, January 1998, through 1.0.6, March 20, 2000, are Copyright (c) 1998, 1999 Glenn Randers-Pehrson, and are distributed according to the same disclaimer and license as libpng-0.96, with the following individuals added to the list of Contributing Authors:

Tom Lane

Glenn Randers-Pehrson

Willem van Schaik

libpng versions 0.89, June 1996, through 0.96, May 1997, are Copyright (c) 1996, 1997 Andreas Dilger Distributed according to the same disclaimer and license as libpng-0.88, with the following individuals added to the list of Contributing Authors:

John Bowler

Kevin Bracey

Sam Bushell

Magnus Holmgren

Greg Roelofs

Tom Tanner

libpng versions 0.5, May 1995, through 0.88, January 1996, are Copyright (c) 1995, 1996 Guy Eric Schalnat, Group 42, Inc.

For the purposes of this copyright and license, "Contributing Authors" is defined as the following set of individuals:

Andreas Dilger

Dave Martindale

Guy Eric Schalnat

Paul Schmidt

Tim Wegner

The PNG Reference Library is supplied "AS IS". The Contributing Authors and Group 42, Inc. disclaim all warranties, expressed or implied, including, without limitation, the warranties of merchantability and of fitness for any purpose. The Contributing Authors and Group 42, Inc. assume no liability for direct, indirect, incidental, special, exemplary, or consequential damages, which may result from the use of the PNG Reference Library, even if advised of the possibility of such damage.

Permission is hereby granted to use, copy, modify, and distribute this source code, or portions hereof, for any purpose, without fee, subject to the following restrictions:

1. The origin of this source code must not be misrepresented.

2. Altered versions must be plainly marked as such and must not be misrepresented as being the original source.

3. This Copyright notice may not be removed or altered from any source or altered source distribution.

The Contributing Authors and Group 42, Inc. specifically permit, without fee, and encourage the use of this source code as a component to supporting the PNG file format in commercial products. If you use this source code in a product, acknowledgment is not required but would be appreciated.

A "png_get_copyright" function is available, for convenient use in "about" boxes and the like:

```
printf("%s",png_get_copyright(NULL));
```

Also, the PNG logo (in PNG format, of course) is supplied in the files "pngbar.png" and "pngbar.jpg" (88x31) and "pngnow.png" (98x31).

Libpng is OSI Certified Open Source Software. OSI Certified Open Source is a

certification mark of the Open Source Initiative.

Glenn Randers-Pehrson

glennrp at users.sourceforge.net

August 13, 2009

BIBLIOTHEK LIBJPEG-6B

Bei der Entwicklung des Programms wurde die Bibliothek libjpeg-6b verwendet.

Copyright (C) 1991-2009, Thomas G. Lane, Guido Vollbeding

LEGAL ISSUES

==========

In plain English:

1. We don't promise that this software works. (But if you find any bugs, please let us know!)

2. You can use this software for whatever you want. You don't have to pay us.

3. You may not pretend that you wrote this software. If you use it in a program, you must acknowledge somewhere in your documentation that you've used the IJG code.

In legalese:

The authors make NO WARRANTY or representation, either express or implied, with respect to this software, its quality, accuracy, merchantability, or fitness for a particular purpose. This software is provided "AS IS", and you, its user, assume the entire risk as to its quality and accuracy.

This software is copyright (C) 1991-2009, Thomas G. Lane, Guido Vollbeding.

All Rights Reserved except as specified below.

Permission is hereby granted to use, copy, modify, and distribute this software (or portions thereof) for any purpose, without fee, subject to these conditions:

(1) If any part of the source code for this software is distributed, then this

README file must be included, with this copyright and no-warranty notice unaltered; and any additions, deletions, or changes to the original files must be clearly indicated in accompanying documentation.

(2) If only executable code is distributed, then the accompanying documentation must state that "this software is based in part on the work of the Independent JPEG Group".

(3) Permission for use of this software is granted only if the user accepts full responsibility for any undesirable consequences; the authors accept NO LIABILITY for damages of any kind.

These conditions apply to any software derived from or based on the IJG code,

not just to the unmodified library. If you use our work, you ought to acknowledge us.

Permission is NOT granted for the use of any IJG author's name or company name

in advertising or publicity relating to this software or products derived from

it. This software may be referred to only as "the Independent JPEG Group's

software".

We specifically permit and encourage the use of this software as the basis of

commercial products, provided that all warranty or liability claims are assumed by the product vendor.

ansi2knr.c is included in this distribution by permission of L. Peter Deutsch,

sole proprietor of its copyright holder, Aladdin Enterprises of Menlo Park, CA.

ansi2knr.c is NOT covered by the above copyright and conditions, but instead

by the usual distribution terms of the Free Software Foundation; principally,

that you must include source code if you redistribute it. (See the file

ansi2knr.c for full details.) However, since ansi2knr.c is not needed as part

of any program generated from the IJG code, this does not limit you more than

the foregoing paragraphs do.

The Unix configuration script "configure" was produced with GNU Autoconf.

It is copyright by the Free Software Foundation but is freely distributable.

The same holds for its supporting scripts (config.guess, config.sub, ltmain.sh). Another support script, install-sh, is copyright by X Consortium

but is also freely distributable.

The IJG distribution formerly included code to read and write GIF files.

To avoid entanglement with the Unisys LZW patent, GIF reading support has

been removed altogether, and the GIF writer has been simplified to produce

"uncompressed GIFs". This technique does not use the LZW algorithm; the

resulting GIF files are larger than usual, but are readable by all standard

GIF decoders.

We are required to state that

> "The Graphics Interchange Format(c) is the Copyright property of
>
> CompuServe Incorporated. GIF(sm) is a Service Mark property of
>
> CompuServe Incorporated."

BIBLIOTHEK LIBUNGIF-4.1.4

Bei der Entwicklung des Programms wurde die Bibliothek libungif-4.1.4 verwendet.

BIBLIOTHEK MD5 MESSAGE-DIGEST ALGORITHM-REV. 2

Bei der Entwicklung des Programms wurde die Bibliothek MD5 MESSAGE-DIGEST ALGORITHM-REV.2 verwendet.

BIBLIOTHEK MD5 MESSAGE-DIGEST ALGORITHM-V. 18.11.2004

Bei der Entwicklung des Programms wurde die Bibliothek MD5 MESSAGE-DIGEST ALGORITHM-V. 18.11.2004 verwendet.

BIBLIOTHEK INDEPENDENT IMPLEMENTATION OF MD5 (RFC 1321)-V. 04.11.1999

Bei der Entwicklung des Programms wurde die Bibliothek Independent implementation of MD5 (RFC 1321)-v verwendet. 04.11.1999.

BIBLIOTHEK CONVERSION ROUTINES BETWEEN UTF32, UTF-16, AND UTF-8-V. 02.11.2004

Bei der Entwicklung des Programms wurde die Bibliothek Conversion routines between UTF32, UTF-16, and UTF-8-v verwendet. 02.11.2004.

BIBLIOTHEK COOL OWNER DRAWN MENUS-V. 2.4, 2.63 BY BRENT CORKUM

Bei der Entwicklung des Programms wurde die Bibliothek Cool Owner Drawn Menus-v verwendet. 2.4, 2.63 By Brent Corkum.

BIBLIOTHEK PLATFORM INDEPENDENT IMAGE CLASS

Bei der Entwicklung des Programms wurde die Bibliothek Platform Independent Image Class verwendet.

Permission is hereby granted to use, copy, modify, and distribute this source code, or portions hereof, for any purpose, including commercial applications, freely and without fee, subject to the following restrictions:

1. The origin of this software must not be misrepresented; you must not claim that you wrote the original software. If you use this software in a product, an acknowledgment in the product documentation would be appreciated but is not required.

2. Altered source versions must be plainly marked as such, and must not be misrepresented as being the original software.

3. This notice may not be removed or altered from any source distribution.

BIBLIOTHEK FLEX PARSER (FLEXLEXER)-V. 1993

Bei der Entwicklung des Programms wurde die Bibliothek Flex parser (FlexLexer)-v verwendet. 1993.

Copyright (c) 1993 The Regents of the University of California

---

This code is derived from software contributed to Berkeley by

Kent Williams and Tom Epperly.

Redistribution and use in source and binary forms with or without modification are permitted provided that: (1) source distributions retain this entire copyright notice and comment, and (2) distributions including binaries display the following acknowledgement: ``This product includes software developed by the University of California, Berkeley and its contributors'' in the documentation or other materials provided with the distribution and in all advertising materials mentioning features or use of this software. Neither the name of the University nor the names of its contributors may be used to endorse or promote products derived from this software without specific prior written permission.

THIS SOFTWARE IS PROVIDED ``AS IS'' AND WITHOUT ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, WITHOUT LIMITATION, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE.

This file defines FlexLexer, an abstract class which specifies the external interface provided to flex C++ lexer objects, and yyFlexLexer, which defines a particular lexer class.

BIBLIOTHEK ENSURECLEANUP, SWMRG, LAYOUT-V. 2000

Bei der Entwicklung des Programms wurde die Bibliothek EnsureCleanup, SWMRG, Layout-v verwendet. 2000.

Copyright (C) 2009, Microsoft Corporation

NOTICE SPECIFIC TO SOFTWARE AVAILABLE ON THIS WEB SITE.

All Software is the copyrighted work of Microsoft and/or its suppliers. Use of the Software is governed by the terms of the end user license agreement, if any, which accompanies or is included with the Software ("License Agreement").

If Microsoft makes Software available on this Web Site without a License Agreement, you may use such Software to design, develop and test your programs to run on Microsoft products and services.

If Microsoft makes any code marked as "sample" available on this Web Site without a License Agreement, then that code is licensed to you under the terms of the Microsoft Limited Public License http://msdn.microsoft.com/en-us/cc300389.aspx#MLPL.

The Software is made available for download solely for use by end users according to the License Agreement or these TOU. Any reproduction or redistribution of the Software not in accordance with the License Agreement or these TOU is expressly prohibited.

WITHOUT LIMITING THE FOREGOING, COPYING OR REPRODUCTION OF THE SOFTWARE TO ANY OTHER SERVER OR LOCATION FOR FURTHER REPRODUCTION OR REDISTRIBUTION IS EXPRESSLY PROHIBITED, UNLESS SUCH REPRODUCTION OR REDISTRIBUTION IS EXPRESSLY PERMITTED BY THE LICENSE AGREEMENT ACCOMPANYING SUCH SOFTWARE.

FOR YOUR CONVENIENCE, MICROSOFT MAY MAKE AVAILABLE ON THIS WEB SITE, TOOLS AND UTILITIES FOR USE AND/OR DOWNLOAD. MICROSOFT DOES NOT MAKE ANY ASSURANCES WITH REGARD TO THE ACCURACY OF THE RESULTS OR OUTPUT THAT DERIVES FROM SUCH USE OF ANY SUCH TOOLS AND UTILITIES. PLEASE RESPECT THE INTELLECTUAL PROPERTY RIGHTS OF OTHERS WHEN USING THE TOOLS AND UTILITIES MADE AVAILABLE ON THIS WEB SITE.

RESTRICTED RIGHTS LEGEND. Any Software which is downloaded from the Web Site for or on behalf of the United States of America, its agencies and/or instrumentalities ("U.S. Government"), is provided with Restricted Rights. Use, duplication, or disclosure by the U.S. Government is subject to restrictions as set forth in subparagraph (c)(1)(ii) of the Rights in Technical Data and Computer Software clause at DFARS 252.227-7013 or subparagraphs (c)(1) and (2) of the Commercial Computer Software - Restricted Rights at 48 CFR 52.227-19, as applicable. Manufacturer is Microsoft Corporation, One Microsoft Way, Redmond, WA 98052-6399.

BIBLIOTHEK STDSTRING- V. 1999

Bei der Entwicklung des Programms wurde die Bibliothek StdString- v verwendet. 1999.

Copyright (C) 1999, Joseph M. O'Leary

This code is free. Use it anywhere you want.

Rewrite it, restructure it, whatever. Please don't blame me if it makes

your $30 billion dollar satellite explode in orbit. If you redistribute

it in any form, I'd appreciate it if you would leave this notice here.

BIBLIOTHEK T-REX (TINY REGULAR EXPRESSION LIBRARY)- V. 2003-2006

Bei der Entwicklung des Programms wurde die Bibliothek T-Rex (tiny regular expression library)- v verwendet. 2003-2006.

Copyright (C) 2003-2006, Alberto Demichelis

This software is provided 'as-is', without any express or implied warranty. In no event will the authors be held liable for any damages arising from the use of this software.

Permission is granted to anyone to use this software for any purpose, including commercial applications, and to alter it and redistribute it freely, subject to the following restrictions:

1. The origin of this software must not be misrepresented; you must not claim that you wrote the original software. If you use this software in a product, an acknowledgment in the product documentation would be appreciated but is not required.

2. Altered source versions must be plainly marked as such, and must not be misrepresented as being the original software.

3. This notice may not be removed or altered from any source distribution.

BIBLIOTHEK NTSERVICE- V. 1997

Bei der Entwicklung des Programms wurde die Bibliothek NTService- v verwendet. 1997.

Copyright (C) 1997, Joerg Koenig and the ADG mbH, Mannheim, Germany

---

Distribute freely, except: don't remove my name from the source or documentation (don't take credit for my work), mark your changes (don't get me blamed for your possible bugs), don't alter or remove this notice.

No warrantee of any kind, express or implied, is included with this software; use at your own risk, responsibility for damages (if any) to anyone resulting from the use of this software rests entirely with the user.

Send bug reports, bug fixes, enhancements, requests, flames, etc., and I'll try to keep a version up to date. I can be reached as follows:

J.Koenig@adg.de (company site)

Joerg.Koenig@rhein-neckar.de (private site)

MODIFIED BY TODD C. WILSON FOR THE ROAD RUNNER NT LOGIN SERVICE.

HOWEVER, THESE MODIFICATIONS ARE BROADER IN SCOPE AND USAGE AND CAN BE USED IN OTHER PROJECTS WITH NO CHANGES.

MODIFIED LINES FLAGGED/BRACKETED BY "//!! TCW MOD"

BIBLIOTHEK SHA-1-1.2

Bei der Entwicklung des Programms wurde die Bibliothek SHA-1-1.2 verwendet.

Copyright (C) 2001, The Internet Society

This document and translations of it may be copied and furnished to others, and derivative works that comment on or otherwise explain it or assist in its implementation may be prepared, copied, published and distributed, in whole or in part, without restriction of any kind, provided that the above copyright notice and this paragraph are included on all such copies and derivative works. However, this document itself may not be modified in any way, such as by removing the copyright notice or references to the Internet Society or other Internet organizations, except as needed for the purpose of developing Internet standards in which case the procedures for copyrights defined in the Internet Standards process must be followed, or as required to translate it into languages other than English.

The limited permissions granted above are perpetual and will not be revoked by the Internet Society or its successors or assigns.

This document and the information contained herein is provided on an "AS IS" basis and THE INTERNET SOCIETY AND THE INTERNET ENGINEERING TASK FORCE DISCLAIMS ALL WARRANTIES, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO ANY WARRANTY THAT THE USE OF THE INFORMATION HEREIN WILL NOT INFRINGE ANY RIGHTS OR ANY IMPLIED WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE.

BIBLIOTHEK COCOA SAMPLE CODE- V. 18.07.2007

Bei der Entwicklung des Programms wurde die Bibliothek Cocoa sample code- v verwendet. 18.07.2007.

BIBLIOTHEK PUTTY SOURCES-25.09.2008

Bei der Entwicklung des Programms wurde die Bibliothek PUTTY SOURCES-25.09.2008 verwendet.

THE SOFTWARE IS PROVIDED "AS IS", WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO THE WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT. IN NO EVENT SHALL SIMON TATHAM BE LIABLE FOR ANY CLAIM, DAMAGES OR OTHER LIABILITY, WHETHER IN AN ACTION OF CONTRACT, TORT OR OTHERWISE, ARISING FROM, OUT OF OR IN CONNECTION WITH THE SOFTWARE OR THE USE OR OTHER DEALINGS IN THE SOFTWARE.

In particular, anybody (even companies) can use PuTTY without restriction (even for commercial purposes) and owe nothing to me or anybody else. Also, apart from having to maintain the copyright notice and the licence text in derivative products, anybody (even companies) can adapt the PuTTY source code into their own programs and products (even commercial products) and owe nothing to me or anybody else. And, of course, there is no warranty and if PuTTY causes you damage you're on your own, so don't use it if you're unhappy with that.

In particular, note that the MIT licence is compatible with the GNU GPL. So if you want to incorporate PuTTY or pieces of PuTTY into a GPL program, there's no problem with that.

ANDERE INFORMATIONEN

Für die Überprüfung elektronischer digitaler Signaturen wird die Krypto-Bibliothek (Programmbibliothek zum Informationsschutz - PBSI) "Crypto C" verwendet, die von CryptoEx OOO, http://www.cryptoex.ru, entwickelt wurde.

Zur Überprüfung der elektronischen digitalen Signatur wird die Programmbibliothek für den Informationsschutz (PBSI) "Agava-C" eingesetzt, die von OOO R-Alpha entwickelt wurde.

Die Software kann Software-Programme enthalten, für die der Nutzer eine (Unter-) Lizenz gemäß der GNU General Public License (GPL) bzw. ähnliche kostenlose Software-Lizenzen erhalten hat, die den Nutzer unter anderem dazu berechtigen, bestimmte Programme oder Teile davon zu kopieren, zu ändern und weiterzugeben und die den Zugang zum Quellcode gestatten ("Open Source Software"). Sofern diese Lizenzen erfordern, dass der Quellcode für eine in einem ausführbaren, binären Format weitergegebene Software dem Nutzer ebenfalls zugänglich gemacht wird, wird der Quellcode nach einer entsprechenden Anforderung an source@kaspersky.com zur Verfügung gestellt bzw. mit der Software geliefert.

GLOSSAR

A

Aktive Lizenz

Lizenz, die momentan für die Arbeit des Kaspersky-Lab-Programms verwendet wird. Die Lizenz legt die Gültigkeitsdauer für den vollen Funktionsumfang sowie die Lizenzpolitik für das Programm fest. Im Programm kann nur ein Schlüssel den Status "aktiv" besitzen.

Archiv

Datei, die ein oder mehrere Objekte "enthält", die ihrerseits auch Archive sein können.

Ausnahme

Eine Ausnahme ist ein Objekt, das von der Untersuchung durch das Kaspersky-Lab-Programm ausgeschlossen wird. Von der Untersuchung können ausgeschlossen werden: Dateien eines bestimmten Formats, Dateien nach Maske, bestimmte Bereiche (beispielsweise ein Ordner oder Programm) sowie Programmprozesse oder Objekte gemäß der Klassifikation der Viren-Enzyklopädie. Für jede Aufgabe können individuelle Ausnahmen festgelegt werden.

Autostart-Objekte

Auswahl von Programmen, die für den Start und die korrekte Funktion des auf Ihrem Computer installierten Betriebssystems und der vorhandenen Software erforderlich sind. Diese Objekte werden jedes Mal beim Hochfahren des Betriebssystems gestartet. Es gibt Viren, die speziell diese Objekte infizieren können. Dadurch kann beispielsweise das Hochfahren des Betriebssystems blockiert werden.

B

Backup

Spezieller Speicher für Sicherungskopien von Objekten, die vor einer Desinfektion oder vor dem Löschen angelegt werden.

Blockieren eines Objekts

Der Zugriff externer Programme auf ein Objekt wird verboten. Ein blockiertes Objekt kann nicht gelesen, ausgeführt, verändert oder gelöscht werden.

Bootvirus

Virus, der die Bootsektoren von Computerlaufwerken infiziert. Der Virus "zwingt" das System beim Hochfahren, nicht auf den eigentlichen Bootcode zuzugreifen, sondern auf den Viruscode, der dann die Kontrolle übernimmt.

D

Dateimaske

Eine Dateimaske ist ein aus allgemeinen Zeichen bestehender Platzhalter für den Namen und die Erweiterung einer Datei. Die zwei wichtigsten Zeichen, die in Dateimasken verwendet werden sind * und ? (wobei * für eine beliebige Anzahl von Zeichen und ? für ein beliebiges Einzelzeichen steht). Mit Hilfe dieser Zeichen kann jede beliebige Datei dargestellt werden. Beachten Sie, dass Name und Endung einer Datei stets durch einen Punkt getrennt werden.

Datenbank-Update

Eine Funktion, die vom Kaspersky-Lab-Programm ausgeführt wird und die es erlaubt, den aktuellen Zustand des Schutzes aufrecht zu erhalten. Dabei werden die Datenbanken von den Kaspersky-Lab-Updateservern auf den Computer kopiert und automatisch von der Anwendung übernommen.

DATENBANKEN

Datenbanken, die von den Kaspersky-Lab-Spezialisten gepflegt werden und eine genaue Beschreibung aller momentan existierenden Bedrohungen der Computersicherheit sowie Methoden zu ihrer Identifikation und Desinfektion enthalten. Die Datenbanken werden von Kaspersky Lab laufend aktualisiert, wenn neue Bedrohungen auftauchen. Um die Erkennungsqualität für Bedrohungen zu steigern, empfehlen wir, regelmäßig Updates für die Datenbanken von den Kaspersky-Lab-Updateservern herunterzuladen.

DATENORDNER

Ordner zum Speichern von für die Arbeit der Anwendung notwendigen Dienstordnern und Datenbanken. Wenn ein Datenordner verändert wird, müssen alle darin gespeicherten Informationen unter der neuen Adresse gespeichert werden.

DESINFEKTION VON OBJEKTEN

Methode zur Verarbeitung von infizierten Objekten, bei der die Daten vollständig oder teilweise wiederhergestellt werden oder eine Entscheidung darüber getroffen wird, dass die Desinfektion von Objekten nicht möglich ist. Die Desinfektion von Objekten erfolgt auf Basis der Einträge in den Datenbänken. Wenn die Desinfektion als primäre Aktion für ein Objekt gilt (erste Aktion mit dem Objekt, die sofort nach seinem Fund ausgeführt wird), wird eine Sicherungskopie des Objekts angelegt, bevor die Desinfektion ausgeführt wird. Bei der Desinfektion können Daten teilweise verloren gehen. Sie können diese Kopie verwenden, um ein Objekt in dem Zustand wiederherzustellen, wie vor der Desinfektion.

DESINFEKTION VON OBJEKTEN BEIM NEUSTART

Methode zur Verarbeitung von infizierten Objekten, die im Augenblick der Desinfektion von anderen Programmen verwendet werden. Dabei wird eine Kopie des infizierten Objekts angelegt. Beim folgenden Neustart wird die Kopie desinfiziert und das infizierte Originalobjekt wird durch die desinfizierte Kopie ersetzt.

DRINGENDES UPDATE

Kritisches Update für die Module des Kaspersky-Lab-Programms.

E

ECHTZEITSCHUTZ

Funktionsmodus des Programms, in dem Objekte im Echtzeitmodus auf schädlichen Code untersucht werden.

Das Programm fängt jeden Versuch zum Öffnen, Schreiben und Ausführen eines Objekts ab, und durchsucht das Objekt nach Bedrohungen. Virenfreie Objekte werden für den Zugriff freigegeben, infizierte oder verdächtige Objekte werden gemäß den Aufgabenparametern verarbeitet (desinfiziert, gelöscht, in die Quarantäne verschoben).

EMPFOHLENE STUFE

Sicherheitsstufe, deren Funktionsparameter von Kaspersky Lab empfohlen werden und die einen optimalen Schutz Ihres Computers gewährleistet. Diese Stufe wird in der Grundeinstellung verwendet.

F

FEHLALARM

Situation, in der ein virenfreies Objekt von der Kaspersky-Lab-Anwendung als infiziert eingestuft wird, weil sein Code Ähnlichkeit mit einem Virus aufweist.

G

GEFÄHRLICHES OBJEKT

Objekt, in dem sich ein Virus befindet. Es wird davor gewarnt, mit solchen Objekten zu arbeiten, weil dies zur Infektion des Computers führen kann. Beim Fund eines infizierten Objekts wird empfohlen, das Objekt mit Hilfe des Kaspersky-Lab-Programms zu desinfizieren oder, falls die Desinfektion nicht möglich ist, es zu löschen.

GEPACKTE DATEI

Archivdatei, die ein Extrahierprogramm und für das Betriebssystem bestimmte Extrahierbefehle enthält.

GEWÖHNLICHES OBJEKT

Körper oder einfacher Anhang einer E-Mail, z.B. in Form einer ausführbaren Datei. Siehe auch Container-Objekt.

GÜLTIGKEITSDAUER DER LIZENZ

Zeitraum, für den Sie berechtigt sind, das Kaspersky-Lab-Programm mit allen Funktionen zu nutzen. Die Gültigkeitsdauer der Lizenz beträgt in der Regel ein Kalenderjahr ab der Installation der Lizenz. Wenn die Gültigkeitsdauer der Lizenz abgelaufen ist, wird die Funktionalität des Programms eingeschränkt: Das Update der Datenbanken ist nicht mehr verfügbar.

H

HEURISTISCHE ANALYSE

Technologie zum Erkennen von Bedrohungen, die sich nicht mit Hilfe der Datenbanken von Anti-Virus identifizieren lassen. Es wird erlaubt, Objekte zu finden, die verdächtig sind, durch einen unbekannten Virus oder eine neue Modifikation eines bekannten Virus infizierte zu sein.

Mit Hilfe der heuristischen Analyse werden bis zu 92 % der neuen Bedrohungen erkannt. Dieser Mechanismus ist sehr effektiv und führt nur selten zu Fehlalarmen.

Dateien, die mit Hilfe der heuristischen Analyse gefunden werden, nennt man verdächtig.

I

ICHECKER-TECHNOLOGIE

Diese Technologie erlaubt eine Erhöhung der Untersuchungsgeschwindigkeit. Dabei werden jene Objekte von der Untersuchung ausgeschlossen, die seit dem vorherigen Scannen nicht verändert wurden, wobei vorausgesetzt wird, dass die Untersuchungsparameter (Antiviren-Datenbanken und Einstellungen) gleich geblieben sind. Informationen darüber werden in einer speziellen Datenbank aufgezeichnet. Die Technologie wird sowohl für den Echtzeitschutz als auch für den Scan auf Befehl verwendet.

Wurde beispielsweise eine Archivdatei vom Programm untersucht und ihr wurde der Status virenfrei zugewiesen. Dann wird das Archiv von der folgenden Untersuchung ausgeschlossen, wenn es nicht verändert wurde und die Untersuchungsparameter gleich geblieben sind. Wenn seit der letzten Untersuchung die Zusammensetzung des Archivs durch Hinzufügen eines neuen Objekts verändert wurde, die Untersuchungsparameter geändert oder die Programm-Datenbanken aktualisiert wurden, wird das Archiv erneut untersucht.

Einschränkungen der Technologie iChecker:

- Die Technologie funktioniert nicht mit großen Dateien, da die Untersuchung der gesamten Datei in diesem Fall weniger Zeit beansprucht, als zu ermitteln, ob sie seit der letzten Untersuchung verändert wurde.

- Die Technologie unterstützt eine begrenzte Anzahl von Formaten (exe, dll, lnk, ttf, inf, sys, com, chm, zip, rar).

INFIZIERTES OBJEKT

Objekt, das schädlichen Code enthält: Bei der Untersuchung des Objekts wurde erkannt, dass ein Abschnitt des Objektcodes vollständig mit dem Code einer bekannten Bedrohung übereinstimmt. Die Kaspersky-Lab-Spezialisten warnen davor, mit solchen Objekten zu arbeiten, weil dies zur Infektion Ihres Computers führen kann.

INKOMPATIBLES PROGRAMM

Antiviren-Programm eines anderen Herstellers oder Programm von Kaspersky Lab, das nicht mit Kaspersky Anti-Virus verwaltet werden kann.

INTERCEPTOR

Subkomponente des Programms, die für die Untersuchung bestimmter Typen von E-Mails verantwortlich ist. Die Auswahl der zu installierenden Interceptoren ist davon abhängig, in welcher Rolle oder Rollenkombination das Programm eingesetzt werden soll.

K

KASPERSKY-LAB-UPDATESERVER

Liste der http- und ftp-Server von Kaspersky Lab, von denen das Programm die Updates für Datenbanken und Module auf Ihren Computer herunterlädt.

KONTROLLIERTES OBJEKT

Datei, die mit den Protokollen HTTP, FTP oder SMTP übertragen und von der Firewall zur Untersuchung durch das Kaspersky-Lab-Programm umgeleitet wird.

KOPFZEILE (HEADER)

Informationen, die am Anfang einer Datei oder E-Mail stehen und Basisdaten über Status und Verarbeitung der Datei (E-Mail) enthalten. Die Kopfzeile einer E-Mail enthält Angaben wie Absender, Empfänger und Datum.

L

LAUFWERKSBOOTSEKTOR

Ein Bootsektor ist ein spezieller Sektor auf der Festplatte eines Computers, auf einer Diskette oder auf einem anderen Gerät zur Datenspeicherung. Er enthält Angaben über das Dateisystem des Datenträgers und ein Bootprogramm, das für den Start des Betriebssystems verantwortlich ist.

Laufwerksbootsektoren können von so genannten Bootviren infiziert werden. Die Kaspersky-Lab-Anwendung erlaubt es, Bootsektoren auf Viren zu untersuchen und infizierte Sektoren zu desinfizieren.

LÖSCHEN EINER E-MAIL

Verarbeitungsmethode für eine E-Mail, die Spam-Merkmale aufweist. Dabei wird die Nachricht physikalisch gelöscht. Diese Methode wird für E-Mails empfohlen, die eindeutig als Spam gelten. Vor dem Löschen einer Nachricht, wird ihre Kopie im Backup gespeichert (wenn diese Funktion nicht deaktiviert wurde).

LÖSCHEN EINES OBJEKTS

Methode zur Objektbearbeitung, bei der das Objekt physikalisch von dem Ort gelöscht wird, an dem es vom Programm gefunden wurde (Festplatte, Ordner, Netzwerkressource). Diese Verarbeitungsmethode wird für gefährliche Objekte empfohlen, deren Desinfektion aus bestimmten Gründen nicht möglich ist.

M

MAXIMALER SCHUTZ

Sicherheitsstufe, die Ihrem Computer den maximalen Schutz bietet, den die Anwendung gewährleisten kann. Auf dieser Sicherheitsstufe werden alle Dateien des Computers sowie Wechseldatenträger und Netzlaufwerke auf Viren untersucht.

MÖGLICHERWEISE INFIZIERTES OBJEKT

Objekt, dessen Code entweder den modifizierten Code eines bekannten Virus oder einen Code, der einem Virus gleicht, enthält, der Kaspersky Lab aber bisher nicht bekannt ist. Infizierte Dateien können mit Hilfe der heuristischen Analyse gefunden werden.

O

OLE-OBJEKT

Objekt, das an eine andere Datei angehängt oder darin eingebettet ist. Das Kaspersky-Lab-Programm erlaubt es, OLE-Objekte auf das Vorhandensein von Viren zu untersuchen. Wenn Sie beispielsweise eine beliebige Tabelle aus Microsoft Office Excel in ein Dokument des Typs Microsoft Office Word einfügen, wird die Tabelle als OLE-Objekt untersucht.

P

POTENTIELL INFIZIERBARES OBJEKT

Ein Objekt das aufgrund seiner Struktur seines Formats von einem Angreifer als "Container" benutzt werden kann, um ein schädliches Objekt zu platzieren oder weiterzuverbreiten. In der Regel sind dies ausführbare Dateien mit Erweiterungen wie com, exe, dll usw. Das Risiko des Eindringens und der Aktivierung von schädlichem Code ist für solche Dateien relativ hoch.

PRIORITÄTSSTUFE FÜR EIN EREIGNIS

Merkmal eines Ereignisses, das bei der Arbeit der Kaspersky-Lab-Anwendung eingetreten ist. Es gibt vier Prioritätsstufen:

- **Kritisches Ereignis.**
- **Funktionsstörung.**
- **Warnung.**
- **Informative Meldung.**

Ereignisse des gleichen Typs können unterschiedliche Prioritätsstufen besitzen. Entscheidend ist die Situation, in der ein Ereignis eintritt.

Q

QUARANTÄNE

Ein bestimmter Ordner, in den alle möglicherweise infizierten Objekte verschoben werden, die bei der Untersuchung oder im Rahmen des Echtzeitschutzes gefunden werden.

R

RESERVELIZENZ

Lizenz, die für die Arbeit der Kaspersky-Lab-Anwendung hinzugefügt, aber nicht aktiviert wurde. Die Reservelizenz wird aktiviert, wenn die Gültigkeit der aktiven Lizenz abläuft.

S

SCHLÜSSELDATEI

Datei mit der Endung .key, die Ihr persönlicher "Schlüssel" ist und für die Arbeit des Kaspersky-Lab-Programms erforderlich ist. Eine Schlüsseldatei ist im Lieferumfang des Produkts enthalten, wenn es bei einem Händler von Kaspersky Lab erworben wurde, oder sie wird Ihnen per E-Mail zugesandt, wenn das Produkt in einem Internetshop gekauft wurde.

SCHUTZSTATUS

Aktueller Schutzstatus, der das Sicherheitsniveau des Computers charakterisiert.

SCHWARZE LISTE FÜR SCHLÜSSELDATEIEN

Datenbank, die Informationen über von Kaspersky Lab gesperrte Schlüsseldateien enthält, deren Besitzer gegen die Bedingungen des Lizenzvertrags verstoßen haben, und über Schlüsseldateien, die zwar ausgestellt, aber nicht verkauft oder ersetzt wurden. Die Datei mit der schwarzen Liste ist für die Arbeit von Kaspersky-Lab-Programmen erforderlich. Die Datei wird gemeinsam mit den Datenbanken aktualisiert.

SCHWELLE FÜR VIRENAKTIVITÄT

Maximal zulässige Anzahl von Ereignissen eines bestimmten Typs innerhalb eines festgelegten Zeitraums, deren Überschreitung als erhöhte Virenaktivität und als Anzeichen eines Virenangriffs gilt. Dieser Wert besitzt insbesondere bei Viren-Epidemien große Bedeutung und erlaubt es dem Administrator, rechtzeitig auf drohende Virenangriffe zu reagieren.

SICHERUNGSKOPIEREN

Bevor ein Desinfektionsversuch erfolgt oder die Datei gelöscht wird, legt die Anwendung eine Sicherungskopie an und speichert diese im Backup. Dadurch wird ermöglicht, die Datei bei Bedarf wiederherzustellen, um sie beispielsweise mit aktualisierten Datenbanken zu untersuchen.

SPEICHER FÜR SICHERUNGSKOPIEN

Spezieller Ordner, der dazu dient, Kopien von Daten des Administrationsservers zu speichern, die mit Hilfe eines Backup-Tools angelegt werden.

SUBNETZMASKE

Die Subnetzmaske (auch Netzwerkmaske genannt) und die Netzwerkadresse definieren die Adressen der Computer, die zu einem Netzwerk gehören.

U

UNBEKANNTER VIRUS

Neuer Virus, über den noch keine Informationen in den Datenbanken vorhanden sind. Unbekannte Viren werden mit der heuristischen Analyse erkannt und erhalten den Status möglicherweise infiziert.

UNTERSUCHUNG DER SPEICHER

Untersuchung der auf einem Mailserver gespeicherten E-Mails und des Inhalts gemeinsamer Ordner unter Verwendung der letzten Datenbankversion. Die Untersuchung erfolgt im Hintergrundmodus und kann entweder nach Zeitplan oder manuell gestartet werden. Es werden alle gemeinsamen Ordner und Mailspeicher (mailbox storage) untersucht. Bei der Untersuchung können neue Viren erkannt werden, über die bei der vorherigen Untersuchung noch keine Datenbankeinträge vorhanden waren.

UPDATE

Vorgang, bei dem vorhandene Dateien (Datenbanken oder Programm-Module) durch neue Dateien ersetzt bzw. neue Dateien hinzugefügt werden. Die neuen Dateien werden von den Kaspersky-Lab-Updateservern heruntergeladen.

UPDATEPAKET

Dateipaket zur Softwareaktualisierung, das aus dem Internet kopiert und auf Ihrem Computer installiert wird.

Ü

ÜBERSPRINGEN EINES OBJEKTS

Verarbeitungsmethode, bei der ein Objekt vom Benutzer übersprungen wird, ohne es zu verändern. Wenn für diesen Ereignistyp in den Berichtsparametern das Protokollieren festgelegt wurde, werden Informationen über das gefundene Objekt im Bericht aufgezeichnet.

V

VERDÄCHTIGES OBJEKT

Objekt, dessen Code entweder den modifizierten Code eines bekannten Virus oder einen Code, der einem Virus gleicht, enthält, der Kaspersky Lab aber bisher nicht bekannt ist. Verdächtige Objekte werden unter Einsatz der heuristischen Analyse erkannt.

VERFÜGBARES UPDATE

Updatepaket für die Module einer Kaspersky-Lab-Anwendung, das dringende Updates, die über einen bestimmten Zeitraum gesammelt wurden, sowie Änderungen der Anwendungsarchitektur enthält.

VERSCHIEBEN VON OBJEKTEN IN DIE QUARANTÄNE

Verarbeitungsmethode für ein möglicherweise infiziertes Objekt. Dabei wird der Zugriff auf das Objekt gesperrt und das Objekt wird vom ursprünglichen Speicherort in den Quarantäneordner verschoben. Dort wird es in verschlüsselter Form gespeichert, um eine Infektion auszuschließen. Quarantäneobjekte können unter Verwendung von aktualisierten Antiviren-Datenbanken untersucht, vom Administrator analysiert oder an Kaspersky Lab eingeschickt werden.

VERTRAUENSWÜRDIGER PROZESS

Programmprozess, dessen Dateioperationen im Echtzeitschutz nicht von der Kaspersky-Lab-Anwendung kontrolliert werden. Das bedeutet, dass alle von einem vertrauenswürdigen Prozess gestarteten, geöffneten und gespeicherten Objekte nicht untersucht werden.

VIRENANGRIFF

Eine Reihe zielgerichteter Versuche, einen Computer mit einem Virus zu infizieren.

VIRENSUCHE

Funktionsmodus der Kaspersky-Lab-Anwendung, der vom Benutzer initiiert wird und zur Untersuchung beliebiger Dateien dienen kann.

W

WIEDERHERSTELLUNG

Ein Originalobjekt wird aus der Quarantäne oder aus dem Backup entweder an den ursprünglichen Ort, an dem das Objekt gespeichert war, bevor es in die Quarantäne verschoben, desinfiziert oder gelöscht wurde, oder in einen benutzerdefinierten Ordner verschoben.

ENDNUTZER-LIZENZVERTRAG FÜR KASPERSKY LAB SOFTWARE

WICHTIGER RECHTLICHER HINWEIS AN ALLE NUTZER: LESEN SIE FOLGENDE RECHTLICHE VEREINBARUNG SORGFÄLTIG DURCH, BEVOR SIE DIE SOFTWARE NUTZEN.

INDEM SIE IM LIZENZVERTRAG-FENSTER AUF DIE SCHALTFLÄCHE AKZEPTIEREN KLICKEN ODER EIN ENTSPRECHENDES ZEICHEN BZW. ENTSPRECHENDE ZEICHEN EINGEBEN, ERKLÄREN SIE SICH MIT DER EINHALTUNG DER GESCHÄFTSBEDINGUNGEN DIESES VERTRAGS EINVERSTANDEN. **DIESE AKTION KONSTITUIERT EIN BEKENNTNIS IHRER SIGNATUR UND SIE STIMMEN DIESER VEREINBARUNG, UND DASS SIE EINE PARTEI DIESER VEREINBARUNG WERDEN, ZU UND ERKLÄREN SICH WEITERHIN EINVERSTANDEN, DASS DIESE VEREINBARUNG, WIE JEDWEDE ANDERE SCHRIFTLICHE, AUSGEHANDELTE UND DURCH SIE UNTERZEICHNETE VEREINBARUNG AUCH, VOLLSTRECKBAR IST.** SOLLTEN SIE MIT DEN GESCHÄFTSBEDINGUNGEN DIESER VEREINBARUNG NICHT EINVERSTANDEN SEIN, BEENDEN SIE DIE INSTALLATION DER SOFTWARE BZW. INSTALLIEREN SIE SIE NICHT.

DIE SOFTWARE KANN BEGLEITET WERDEN VON EINER ZUSATZVEREINBARUNG ODER EINEM ÄHNLICHEN DOKUMENT („ZUSATZVEREINBARUNG"), IN DER/DEM DIE ANZAHL DER COMPUTER, AUF DENEN DIE SOFTWARE INSTALLIERT WERDEN DARF, DIE NUTZUNGSDAUER DER SOFTWARE, DIE OBJEKTTYPEN, FÜR DIE DIE SOFTWARE VORGESEHEN IST, UND WEITERE BEDINGUNGEN ZUM KAUF; ERWERB UND GEBRAUCH FESTGELEGT WERDEN. EINE SOLCHE ZUSATZVEREINBARUNG IST EIN BESTANDTEIL DES LIZENZVERTRAGS.

NACHDEM SIE IM LIZENZVERTRAG-FENSTER AUF DIE SCHALTFLÄCHE AKZEPTIEREN GEKLICKT ODER EIN ENTSPRECHENDES ZEICHEN BZW. ENTSPRECHENDE ZEICHEN EINGEGEBEN HABEN, SIND SIE BERECHTIGT, DIE SOFTWARE IM EINKLANG MIT DEN GESCHÄFTSBEDINGUNGEN DIESER VEREINBARUNG ZU NUTZEN.

1. Definitionen

1.1. **Software** bezeichnet Software einschließlich aller Updates und zugehöriger Materialien.

1.2. **Rechtsinhaber** (Inhaber aller Rechte an der Software, ob exklusiv oder anderweitig) bezeichnet Kaspersky Lab ZAO, ein gemäß den Gesetzen der Russischen Föderation amtlich eingetragenes Unternehmen.

1.3. **Computer** bezeichnet/bezeichnen Hardware, einschließlich von PCs, Laptops, Workstations, PDAs, Smart Phones, tragbaren oder sonstigen elektronischen Geräten, für welche die Software konzipiert war und auf denen die Software installiert und/oder verwendet werden wird.

1.4. **Endnutzer (Sie)** bezeichnet eine bzw. mehrere Personen, die die Software in eigenem Namen installieren oder nutzen, oder die eine Software-Kopie rechtmäßig nutzt/nutzen, oder, falls die Software im Namen einer Organisation heruntergeladen oder installiert wurde, wie etwa einem Arbeitgeber, bezeichnet der Begriff *„Sie"* weiterhin jene Organisation, für die die Software heruntergeladen oder installiert wird, und es wird hiermit erklärt, dass eine solche Organisation die diese Vereinbarung akzeptierende Person autorisiert hat, dies in ihrem Namen zu tun. Im Sinne dieses Lizenzvertrags beinhaltet der Begriff *„Organisation"* ohne Einschränkungen jedwede Partnerschaft, GmbH, Gesellschaft, Vereinigung, Aktiengesellschaft, Treuhandgesellschaft, Gemeinschaftsunternehmen, Arbeitsorganisation, nicht eingetragene Organisation oder staatliche Behörde.

1.5. **Partner** bezeichnet Organisationen oder Personen, die die Software auf Grundlage eines Vertrags und einer mit dem Rechtsinhaber vereinbarten Lizenz vertreiben.

1.6. **Update(s)** bezeichnet/n alle Upgrades, Korrekturen, Patches, Erweiterungen, Reparaturen, Modifikationen, Kopien, Ergänzungen oder Wartungs-Softwarepakete usw.

1.7. **Benutzerhandbuch** bezeichnet die Bedienungsanleitung, die Administrator-Anleitung, ein Nachschlagewerk und ähnliche erläuternde oder sonstige Materialien.

1.8. **Software-Anschaffung** bezeichnet den Kauf oder anderweitigen Erwerb der Software gemäß den Bestimmungen in der Zusatzvereinbarung. Dazu zählt auch eine Gratis-Anschaffung der Software.

2. Lizenzgewährung

2.1. Der Rechtsinhaber gewährt Ihnen hiermit eine nicht-ausschließliche Lizenz zur Speicherung, zum Laden, zur Installation, Ausführung und Darstellung (zur „Nutzung") der Software auf einer festgelegten Anzahl von Computern zur Unterstützung des Schutzes Ihres Computers, auf dem die Software installiert ist, vor im Nutzerhandbuch beschriebenen Bedrohungen gemäß den technischen, im Benutzerhandbuch beschriebenen Anforderungen und im Einklang mit den Geschäftsbedingungen dieses Vertrags (die „Lizenz"). Sie erkennen diese Lizenz an.
Testversion. Sollten Sie eine Testversion der Software erhalten, heruntergeladen und/oder installiert haben und sollte Ihnen hiermit eine Evaluierungslizenz für die Software gewährt worden sein, dürfen Sie die Software ab

dem Datum der ersten Installation nur zu Evaluierungszwecken verwenden, und zwar ausschließlich während der einzigen geltenden Evaluierungsperiode, außer wie anderweitig angegeben. Jegliche Nutzung der Software zu anderen Zwecken oder über die geltende Evaluierungsperiode hinaus ist strikt untersagt.

Software für mehrere Umgebungen; Mehrsprachige Software; Dual-Medien-Software; Mehrere Kopien; Softwarebündel. Wenn Sie verschiedene Versionen der Software oder verschiedene Sprachausgaben der Software verwenden, wenn Sie die Software auf mehreren Medien erhalten, wenn Sie anderweitig mehrere Kopien der Software erhalten oder wenn Sie die Software mit einer anderen Software gebündelt erhalten sollten, entspricht die insgesamt zulässige Anzahl Ihrer Computer, auf denen alle Versionen der Software installiert sind, der Anzahl der Computer, wie sie in den Lizenzen angegeben sind, die Sie vom Rechtsinhaber bezogen haben, und jede erworbene Lizenz berechtigt Sie zur Installation und Nutzung der Software auf dieser Anzahl von Computern entsprechend den Festlegungen in den Klauseln 2.2 und 2.3, *außer die* Lizenzbedingungen sehen eine anderweitige Regelung vor.

2.2. Wenn die Software auf einem physischen Medium erworben wurde, haben Sie das Recht, die Software zum Schutz einer solchen Anzahl von Computern zu verwenden, wie sie auf der Softwareverpackung oder in der Zusatzvereinbarung angegeben ist.

2.3. Wenn die Software über das Internet erworben wurde, haben Sie das Recht, die Software zum Schutz einer solchen Anzahl von Computern zu verwenden, wie sie festgelegt wurde, als Sie die Lizenz für die Software gekauft haben, bzw. wie sie in der Zusatzvereinbarung angegeben ist.

2.4. Sie haben das Recht, eine Kopie der Software anzufertigen, und zwar ausschließlich zu Sicherungszwecken und nur, um die rechtmäßig in Ihrem Besitz befindliche Kopie zu ersetzen, sollte eine solche Kopie verloren gehen, zerstört oder unbrauchbar werden. Diese Sicherungskopie kann nicht zu anderen Zwecken verwendet werden und muss zerstört werden, wenn Sie das Recht verlieren, die Software zu nutzen oder wenn Ihre Lizenz abläuft oder aus irgendeinem Grund im Einklang mit der gültigen Gesetzgebung im Land Ihres Wohnsitzes oder in dem Land, in dem Sie die Software nutzen, gekündigt werden sollte.

2.5. Sie können die nicht-exklusive Lizenz zur Nutzung der Software an andere Personen oder Rechtspersönlichkeiten innerhalb des Rahmens der Ihnen vom Rechtsinhaber gewährten Lizenz übertragen, vorausgesetzt, dass der Empfänger allen Geschäftsbedingungen dieses Vertrags zustimmt bzw. bejaht, Sie vollständig in der vom Rechtsinhaber gewährten Lizenz zu vertreten. In dem Fall, dass Sie die vom Rechtsinhaber gewährten Rechte zur Nutzung der Software vollständig übertragen, müssen Sie alle Kopien der Software, und zwar einschließlich der Sicherungskopie, zerstören. Wenn Sie Empfänger einer übertragenen Lizenz sind, müssen Sie zustimmen, alle Geschäftsbedingungen dieses Vertrags einzuhalten. Wenn Sie den Geschäftsbedingungen dieses Vertrags nicht vollständig zustimmen, dürfen Sie die Software nicht installieren und/oder verwenden. Sie stimmen als Empfänger einer übertragenen Lizenz weiterhin zu, dass Sie über keine zusätzlichen oder besseren Rechte verfügen, als der ursprüngliche Endnutzer, der die Software vom Rechtsinhaber erworben hat.

2.6. Ab dem Zeitpunkt der Aktivierung der Software bzw. Installation der Lizenzschlüsseldatei (mit Ausnahme einer Testversion der Software) haben Sie das Recht, folgende Dienstleistungen für den auf der Softwareverpackung (falls Sie Software auf einem physischen Medium erworben haben) oder während des Kaufs (falls die Software über das Internet erworben wurde) festgelegten Zeitraum zu beziehen:

- Updates der Software über das Internet, wenn und wie der Rechtsinhaber diese auf seiner Webseite oder mittels anderer Online-Dienste veröffentlicht. Jedwede Updates, die Sie erhalten, werden Teil der Software und die Geschäftsbedingungen dieses Vertrags gelten für diese;
- Technische Unterstützung über das Internet sowie technische Unterstützung über die Telefon-Hotline.

3. Aktivierung und Zeitraum

3.1. Falls Sie Modifikationen an Ihrem Computer oder an der darauf installierten Software anderer Anbieter vornehmen, kann der Rechtsinhaber von Ihnen verlangen, die Aktivierung der Software bzw. die Installation der Lizenzschlüsseldatei zu wiederholen. Der Rechtsinhaber behält sich das Recht vor, jegliche Mittel und Verifizierungsverfahren zu nutzen, um die Gültigkeit der Lizenz und/oder die Rechtmäßigkeit einer Kopie der Software, die auf Ihrem Computer installiert und/oder genutzt wird, zu verifizieren.

3.2. Falls die Software auf einem physischen Medium erworben wurde, kann die Software nach Ihrer Annahme dieses Vertrags mit Beginn ab dem Zeitpunkt der Annahme dieses Vertrags während des auf der Verpackung bezeichneten oder in der Zusatzvereinbarung angegebenen Zeitraums genutzt werden.

3.3. Falls die Software über das Internet erworben wurde, kann die Software nach Ihrer Annahme dieses Vertrags für die während des Kaufs bezeichnete oder die in der Zusatzvereinbarung angegebene Zeitdauer genutzt werden.

3.4. Sie haben das Recht, eine Testversion der Software zu nutzen, und zwar gemäß der Festlegung in Klausel 2.1 und ohne jedwede Gebühr für die einzelne geltende Evaluierungsperiode (30 Tage) ab dem Zeitpunkt der Aktivierung der Software im Einklang mit diesem Vertrag, *und zwar unter der Bedingung, dass* die Testversion Ihnen nicht das Recht auf Updates und technische Unterstützung über das Internet und technische Unterstützung über die Telefon-Hotline einräumt.

3.5. Ihre Lizenz zur Nutzung der Software beschränkt sich auf den in den Klauseln 3.2 oder 3.3 (je nach Anwendbarkeit) bezeichneten Zeitraum. Die verbleibende Zeitdauer kann auf die im Benutzerhandbuch beschriebene Weise abgefragt werden.

3.6. Haben Sie die Software zur Nutzung auf mehr als einem Computer erworben, beginnt der Zeitraum, auf den Ihre Lizenz zur Nutzung der Software begrenzt ist, am Tag der Aktivierung der Software bzw. der Installation der Lizenzschlüsseldatei auf dem ersten Computer.

3.7. Unbeschadet anderer Rechtsmittel laut Gesetz oder Billigkeitsrecht, zu denen der Rechtsinhaber im Falle eines Verstoßes gegen die Geschäftsbedingungen dieses Vertrags durch Sie berechtigt ist, ist der Rechtsinhaber jederzeit, ohne Sie benachrichtigen zu müssen, dazu berechtigt, diese Lizenz zur Nutzung der Software zu kündigen, und zwar ohne den Verkaufspreis oder einen Teil davon zurückzuerstatten.

3.8. Sie stimmen zu, dass Sie bei der Nutzung der Software sowie bei der Verwendung jedweder Berichte oder Informationen, die sich als Ergebnis der Nutzung der Software ableiten, alle geltenden internationalen, nationalen, staatlichen, regionalen und lokalen Gesetze sowie gesetzlichen Bestimmungen, einschließlich (und ohne Beschränkung) Datenschutz-, Urheber-, Exportkontroll- und Verfassungsrecht, einhalten werden.

3.9. Außer wenn anderweitig hierin festgelegt, dürfen Sie keines der Rechte, die Ihnen unter diesem Vertrag gewährt werden, bzw. keine Ihrer hieraus entstehenden Pflichten übertragen oder abtreten.

4. Technische Unterstützung

Die in Klausel 2.6 dieses Vertrags erläuterte technische Unterstützung wird Ihnen gewährt, wenn das neueste Update der Software installiert wird (außer im Fall einer Testversion der Software).
Technischer Support: http://support.kaspersky.com

5. Sammeln von Informationen

5.1. Durch Zustimmung zu den Geschäftsbedingungen dieses Vertrags haben Sie eingewilligt, dem Rechtsinhaber Informationen über die ausführbaren Dateien und ihre Prüfsummen zur Verfügung zu stellen, um Ihr Sicherheits-Schutzniveau zu verbessern.

5.2. Um das Sicherheitsbewusstsein bezüglich neuer Bedrohungen und deren Quellen zu verbessern, bzw. um Ihr Sicherheits-Schutzniveau zu verbessern, ist der Rechtsinhaber ausdrücklich berechtigt, mit Ihrer Zustimmung, die ausdrücklich in der Kaspersky Security Network Datenerfassungserklärung bestätigt wurde, derartige Informationen zu empfangen. Sie können den Kaspersky Security Network Service während der Installation deaktivieren. Sie können ebenfalls jederzeit auf der Softwareoptionsseite den Kaspersky Security Network Service aktivieren und deaktivieren.

Sie bestätigen und erkennen weiterhin an, dass jedwede Informationen, die vom Rechtsinhaber erfasst werden, zum Zweck der Verfolgung und Veröffentlichung von Sicherheitsrisikotrends verwendet werden können, und zwar nach freiem Ermessen des Rechtsinhabers.

5.3. Die Software verarbeitet keine personenbezogenen Daten und kombiniert keine Verarbeitungsdaten und persönlichen Informationen.

5.4. Sollten Sie nicht wünschen, dass die von der Software gesammelten Informationen an den Rechtsinhaber geschickt werden, sollten Sie den Kaspersky Security Network Service nicht aktivieren und/oder deaktivieren.

6. Beschränkungen

5.1. Sie werden die Software nicht emulieren, klonen, vermieten, verleihen, leasen, verkaufen, modifizieren, dekompilieren oder zurückentwickeln oder disassemblieren oder Arbeiten auf Grundlage der Software oder eines Teils davon ableiten, jedoch mit der einzigen Ausnahme eines Ihnen durch geltende Gesetzgebung gewährten Rechts, von dem keine Rücktretung möglich ist, und Sie werden in keiner anderen Form irgendeinen Teil der Software in menschlich lesbare Form umwandeln oder die lizenzierte Software oder irgendeine Teilmenge der lizenzierten Software übertragen, noch irgendeiner Drittpartei gestatten, dies zu tun, außer im Umfang vorangegangener Einschränkungen, die ausdrücklich durch geltendes Recht untersagt sind. Weder Binärcode noch Quellcode der Software dürfen verwendet oder zurückentwickelt werden, um den Programmalgorithmus, der proprietär ist, wiederherzustellen. Alle Rechte, die nicht ausdrücklich hierin gewährt werden, verbleiben beim Rechtsinhaber und/oder dessen Zulieferern, je nachdem, was zutrifft. Jegliche derartige nicht autorisierte Nutzung der Software kann zur sofortigen und automatischen Kündigung dieses Vertrags sowie der hierunter gewährten Lizenz und zu Ihrer straf- und/oder zivilrechtlichen Verfolgung führen.

5.2. Sie werden die Rechte zur Nutzung der Software nicht an eine Drittpartei übertragen, außer entsprechend der Festlegung in Klausel 2.5 dieses Vertrags.

5.3. Sie werden den Aktivierungscode und/oder die Lizenzschlüssel-Datei keinen Drittparteien verfügbar machen oder Drittparteien Zugang zum Aktivierungscode und/oder zum Lizenzschlüssel gewähren. Aktivierungscode und/oder Lizenzschlüssel werden/wird als vertrauliche Daten des Rechtsinhabers betrachtet, und Sie werden angemessene Sorgfalt zum Schutz der Vertraulichkeit des Aktivierungscodes und/oder des Lizenzschlüssels walten lassen, sofern Sie den Aktivierungscode und/oder den Lizenzschlüssel entsprechend der Festlegung in Klausel 2.5 dieses Vertrags an Drittparteien übertragen dürfen.

5.4. Sie werden die Software nicht an eine Drittpartei vermieten, verleasen oder verleihen.

5.5. Sie werden die Software nicht zur Erstellung von Daten oder Software verwenden, die zur Feststellung, zum Sperren oder zur Handhabung von Bedrohungen, wie im Nutzerhandbuch beschrieben, genutzt werden.

5.6. Der Rechtsinhaber hat das Recht, die Schlüsseldatei zu blockieren oder Ihre Lizenz zu kündigen, falls Sie gegen irgendwelche Geschäftsbedingungen dieses Vertrags verstoßen, und zwar ohne irgendeine Rückerstattung an Sie.

5.7. Falls Sie die Testversion der Software verwenden, sind Sie nicht berechtigt, technische Unterstützung, wie in Klausel 4 dieses Vertrags festgelegt, zu erhalten, und Sie sind ebenfalls nicht berechtigt, die Lizenz oder die Rechte zur Nutzung der Software an irgendeine Drittpartei zu übertragen.

6. Eingeschränkte Garantie und Haftungsausschluss

6.1. Der Rechtsinhaber garantiert, dass die Software im Wesentlichen im Einklang mit den im Nutzerhandbuch dargelegten Spezifikationen und Beschreibungen funktionieren wird, *jedoch vorausgesetzt,* dass eine solche eingeschränkte Garantie nicht für Folgendes gilt: (w) Mängel Ihres Computers und zugehörigen Verstoß, wofür der Rechtsinhaber ausdrücklich jedwede Gewährleistungsverantwortung ablehnt; (x) Funktionsstörungen, Defekte oder Ausfälle, resultierend aus falscher Verwendung, Missbrauch, Unfall, Nachlässigkeit, unsachgemäßer/m Installation, Betrieb oder Wartung, Diebstahl, Vandalismus, höherer Gewalt, terroristischen Akten, Stromausfällen oder -schwankungen, Unglück, Veränderung, nicht zulässiger Modifikation oder Reparaturen durch eine Partei außer dem Rechtsinhaber oder Maßnahmen einer sonstigen Drittpartei oder Aktionen ihrerseits, oder Ursachen außerhalb der Kontrolle des Rechtsinhabers; (y) jedweder Defekt, der dem Rechtsinhaber nicht durch Sie bekannt gemacht wird, sobald dies nach dem ersten Auftreten des Defekts möglich ist; und (z) Inkompatibilität, verursacht durch Hardware- und/oder Software-Komponenten, die auf Ihrem Computer installiert sind.

6.2. Sie bestätigen, akzeptieren und erkennen an, dass keine Software frei von Fehlern ist, und Sie sind angehalten, den Computer mit einer für Sie geeigneten Häufigkeit und Beständigkeit zu sichern.

6.3. Der Rechtsinhaber gibt keine Garantie, dass die Software im Fall von Verstößen gegen die Bedingungen, wie im Nutzerhandbuch oder in diesem Vertrag beschrieben, einwandfrei funktionieren wird.

6.4. Der Rechtsinhaber garantiert nicht, dass die Software einwandfrei funktionieren wird, wenn Sie nicht regelmäßig, wie in Klausel 2.6 dieses Vertrags erläutert, Updates herunterladen.

6.5. Der Rechtsinhaber garantiert keinen Schutz vor im Nutzerhandbuch beschriebenen Bedrohungen nach Ablauf der in Klausel 3.2 oder 3.3 dieses Vertrags bezeichneten Periode oder nachdem die Lizenz zur Nutzung der Software aus irgendeinem Grund gekündigt wurde.

6.6. DIE SOFTWARE WIRD OHNE MÄNGELGEWÄHR BEREITGESTELLT UND DER RECHTSINHABER GIBT KEINE ZUSICHERUNG UND KEINE GEWÄHRLEISTUNG IN BEZUG AUF IHRE NUTZUNG ODER LEISTUNG. DER RECHTSINHABER UND SEINE PARTNER GEWÄHREN AUßER DEN GARANTIEN, ZUSICHERUNGEN, BESTIMMUNGEN ODER BEDINGUNGEN, DIE DURCH GELTENDES RECHT NICHT AUSGESCHLOSSEN ODER BESCHRÄNKT WERDEN KÖNNEN, KEINE GARANTIEN, ZUSICHERUNGEN, BESTIMMUNGEN ODER BEDINGUNGEN (AUSDRÜCKLICHER ODER STILLSCHWEIGENDER NATUR, DIE ENTWEDER AUS EINER GESCHÄFTSBEZIEHUNG ODER EINEM HANDELSBRAUCH ENTSTEHEN BZW. AUS GESETZLICHEN, GEWOHNHEITSRECHTLICHTEN ODER ANDEREN VORSCHRIFTEN ABGELEITET WERDEN) HINSICHTLICH JEDWEDER ANGELEGENHEIT, EINSCHLIEßLICH (OHNE EINSCHRÄNKUNG) VON NICHTVERLETZUNG VON RECHTEN DRITTER, MARKTGÄNGIGKEIT, BEFRIEDIGENDE QUALITÄT, INTEGRIERUNG ODER BRAUCHBARKEIT FÜR EINEN BESTIMMTEN ZWECK. SIE TRAGEN DAS GESAMTE STÖRUNGSRISIKO UND DAS GESAMTRISIKO HINSICHTLICH DER LEISTUNG UND VERANTWORTUNG FÜR DIE AUSWAHL DER SOFTWARE, UM IHRE VORGESEHENEN RESULTATE ZU ERZIELEN, UND FÜR DIE INSTALLATION SOWIE DIE NUTZUNG DER SOFTWARE UND DIE MIT IHR ERZIELTEN ERGEBNISSE. OHNE EINSCHRÄNKUNG DER VORANGEGANGENEN BESTIMMUNGEN MACHT DER RECHTSINHABER KEINE ZUSICHERUNGEN UND GIBT KEINE GEWÄHRLEISTUNG, DASS DIE SOFTWARE FEHLERFREI ODER FREI VON UNTERBRECHUNGEN ODER SONSTIGEN STÖRUNGEN IST ODER DASS DIE SOFTWARE JEDWEDE ODER ALL IHRE ANFORDERUNGEN ERFÜLLEN WIRD, UNGEACHTET DESSEN, OB GEGENÜBER DEM RECHTSINHABER OFFEN GELEGT ODER NICHT.

7. Haftungsausschluss und Haftungsbeschränkungen

INSOWEIT GESETZLICH STATTHAFT, SIND DER RECHTSINHABER UND SEINE PARTNER UNTER KEINEN UMSTÄNDEN HAFTBAR FÜR JEDWEDE SPEZIELLEN ODER BEILÄUFIGEN SCHÄDEN, STRAFZUSCHLAG ZUM SCHADENERSATZ, INDIREKTE ODER FOLGESCHÄDEN (EINSCHLIEßLICH UND NICHT BESCHRÄNKT AUF SCHÄDEN AUS VERLUST VON GEWINN ODER VERTRAULICHEN ODER SONSTIGEN INFORMATIONEN, FÜR GESCHÄFTSUNTERBRECHUNG, FÜR VERLUST VON PRIVATSPHÄRE, KORRUPTION, BESCHÄDIGUNG UND VERLUST VON DATEN ODER PROGRAMMEN, FÜR VERSÄUMNIS EINER PFLICHTERFÜLLUNG, EINSCHLIEßLICH JEDWEDER GESETZLICHER PFLICHTEN, TREUEPFLICHT ODER PFLICHT ZUR WAHRUNG ANGEMESSENER SORGFALT, FÜR NACHLÄSSIGKEIT, FÜR WIRTSCHAFTLICHEN VERLUST UND FÜR FINANZIELLEN ODER JEDWEDEN SONSTIGEN VERLUST), DIE AUS ODER AUF IRGENDEINE WEISE IM ZUSAMMENHANG MIT DER NUTZUNG ODER UNMÖGLICHKEIT DER NUTZUNG DER SOFTWARE, DER BEREITSTELLUNG ODER DEM VERSÄUMNIS DER BEREITSTELLUNG TECHNISCHER UNTERSTÜTZUNG ODER SONSTIGER DIENSTLEISTUNGEN, INFORMATIONEN, SOFTWARE UND ZUGEHÖRIGEM INHALT MITTELS DER SOFTWARE RESULTIEREN, ODER SICH ANDERWEITIG AUS DER NUTZUNG DER SOFTWARE ODER ANDERWEITIG UNTER BZW. IM ZUSAMMENHANG MIT EINER BESTIMMUNG DIESES VERTRAGS ERGEBEN, ODER DIE FOLGE EINES VERTRAGSBRUCHS ODER UNERLAUBTER HANDLUNG (EINSCHLIEßLICH NACHLÄSSIGKEIT, FALSCHANGABE,

JEDWEDER STRIKTEN HAFTUNGSVERPFLICHTUNG ODER -PFLICHT), ODER EINER VERLETZUNG GESETZLICHER PFLICHTEN ODER DER GEWÄHRLEISTUNG DES RECHTSINHABERS ODER EINES SEINER PARTNER SIND, UND ZWAR AUCH DANN NICHT, WENN DER RECHTSINHABER ODER EINER SEINER PARTNER BEZÜGLICH DER MÖGLICHKEIT SOLCHER SCHÄDEN INFORMIERT WURDE.

SIE STIMMEN ZU, DASS IN DEM FALL, DASS DER RECHTSINHABER UND/ODER SEINE PARTNER HAFTBAR GEMACHT WERDEN/WIRD, DIE HAFTUNG DES RECHTSINHABERS UND/ODER SEINER PARTNER AUF DIE KOSTEN DER SOFTWARE BESCHRÄNKT IST. UNTER KEINEN UMSTÄNDEN WIRD DIE HAFTUNG DES RECHTSINHABERS UND/ODER SEINER PARTNER DIE FÜR DIE SOFTWARE ERSTATTETEN KOSTEN AN DEN RECHTSINHABER ODER DEN PARTNER ÜBERSTEIGEN (JE NACHDEM, WAS ZUTRIFFT).

NICHTS IN DIESEM VERTRAG SCHLIEßT EINEN ANSPRUCH AUFGRUND VON TOD UND PERSONENSCHADEN AUS ODER SCHRÄNKT DIESEN EIN. IN DEM FALL, DASS EIN HAFTUNGSAUSSCHLUSS, EIN AUSSCHLUSS ODER EINE EINSCHRÄNKUNG IN DIESEM VERTRAG AUFGRUND GELTENDEN RECHTS NICHT AUSGESCHLOSSEN ODER BESCHRÄNKT WERDEN KANN, WIRD NUR EIN SOLCHER HAFTUNGSAUSSCHLUSS, AUSSCHLUSS ODER EINE EINSCHRÄNKUNG NICHT FÜR SIE GELTEN, UND SIE SIND WEITERHIN AN JEDWEDE VERBLEIBENDEN HAFTUNGSAUSSCHLÜSSE, AUSSCHLÜSSE ODER EINSCHRÄNKUNGEN GEBUNDEN.

8. GNU und sonstige Drittpartei-Lizenzen

Die Software kann einige Softwareprogramme enthalten, die an den Nutzer unter der GPL (GNU General Public License) oder sonstigen vergleichbaren freien Softwarelizenzen lizenziert (oder unterlizenziert) sind und dem Nutzer neben anderen Rechten gestatten, bestimmte Programme oder Teile dieser Programme zu kopieren, zu modifizieren und weiter zu verbreiten und sich Zugang zum Quellcode zu verschaffen („Open Source Software“). Falls es solche Lizenzen erforderlich machen, dass für jedwede Software, die an jemanden in ausführbarem Binärformat geliefert wird, diesen Nutzern der Quellcode ebenfalls verfügbar gemacht wird, dann soll der Quellcode zur Verfügung gestellt werden, indem ein diesbezügliches Ersuchen an source@kaspersky.com gesendet wird, oder der Quellcode wird mit der Software geliefert. Falls irgendwelche Open Source Software-Lizenzen es erforderlich machen, dass der Rechtsinhaber Rechte zur Nutzung, zum Kopieren oder zur Änderung eines Open Source Software-Programms bereitstellt, welche umfassender sind, als die in diesem Vertrag gewährten Rechte, dann werden derartige Rechte Vorrang vor den hierin festgelegten Rechten und Einschränkungen haben.

9. Geistiges Eigentum

10.1 Sie stimmen zu, dass die Software sowie die Urheberschaft, Systeme, Ideen, Betriebsmethoden, Dokumentation und sonstige in der Software enthaltenen Informationen proprietäres geistiges Eigentum und/oder die wertvollen Geschäftsgeheimnisse des Rechtsinhabers oder seiner Partner sind und dass der Rechtsinhaber und seine Partner, je nachdem was zutrifft, durch das Zivil- und Strafrecht sowie durch Gesetze zum Urheberrecht, bezüglich Geschäftsgeheimnissen, Handelsmarken und Patenten der Russischen Föderation, der Europäischen Union und der Vereinigten Staaten sowie anderer Länder und internationaler Übereinkommen geschützt sind. Dieser Vertrag gewährt Ihnen keinerlei Rechte am geistigen Eigentum, einschließlich an jeglichen Handelsmarken und Servicemarken des Rechtsinhabers und/oder seiner Partner („Handelsmarken“). Sie dürfen die Handelsmarken nur so weit nutzen, um von der Software im Einklang mit der akzeptierten Handelsmarkenpraxis erstellte Druckausgaben zu identifizieren, einschließlich der Identifizierung des Namens des Besitzers der Handelsmarke. Eine solche Nutzung der Handelsmarke gibt Ihnen keinerlei Besitzrechte an dieser Handelsmarke. Der Rechtsinhaber und/oder seine Partner besitzen und behalten alle Rechte, Titel und Anteile an der Software, einschließlich (ohne jedwede Einschränkung) jedweden Fehlerkorrekturen, Erweiterungen, Updates oder sonstigen Modifikationen an der Software, ob durch den Rechtsinhaber oder eine beliebige Drittpartei vorgenommen, und allen Urheberrechten, Patenten, Rechten an Geschäftsgeheimnissen, Handelsmarken und sonstigem geistigen Eigentum daran. Ihr Besitz, die Installation oder Nutzung der Software lässt den Titel am geistigen Eigentum an der Software nicht auf Sie übergehen, und Sie erwerben keinerlei Rechte an der Software, außer jene ausdrücklich in diesem Vertrag dargelegten. Alle hierunter erstellten Kopien der Software müssen dieselben proprietären Informationen enthalten, die auf und in der Software erscheinen. Mit Ausnahme der hierin aufgeführten Bestimmungen gewährt Ihnen dieser Vertrag keine Rechte geistigen Eigentums an der Software und Sie bestätigen, dass diese unter diesem Vertrag gewährte Lizenz Ihnen gemäß den weiteren Festlegungen hierin ausschließlich das Recht auf eingeschränkte Nutzung unter den Geschäftsbedingungen dieses Vertrags gewährt. Der Rechtsinhaber behält sich alle Rechte vor, die Ihnen nicht ausdrücklich in diesem Vertrag gewährt wurden.

10.2 Sie bestätigen, dass der Quellcode, der Aktivierungscode und/oder die Lizenzschlüssel-Datei für die Software Eigentum des Rechtsinhabers sind und Geschäftsgeheimnisse des Rechtsinhabers konstituieren. Sie stimmen zu, den Quellcode der Software nicht zu modifizieren, abzuwandeln, zu übersetzen, zurückzuentwickeln, zu dekompilieren oder auf sonstige Weise zu versuchen, den Quellcode ausfindig zu machen.

10.3 Sie stimmen zu, die Software in keinster Weise zu modifizieren oder abzuändern. Sie dürfen die Urheberrechtshinweise oder sonstige proprietäre Hinweise auf jedweden Kopien der Software nicht entfernen oder verändern.

10. Geltendes Recht; Schiedsverfahren

Dieser Vertrag unterliegt den Gesetzen der Russischen Föderation und wird nach diesen ausgelegt, und zwar ohne Bezug auf gegenteilige gesetzliche Regelungen und Prinzipien. Dieser Vertrag wird nicht dem Übereinkommen der Vereinten Nationen über Verträge über den internationalen Warenverkauf unterliegen, dessen Anwendung ausschließlich ausgeschlossen wird. Jede Meinungsverschiedenheit, die aus den Bedingungen dieses Vertrags, deren Auslegung oder Anwendung oder einem Verstoß gegen diese resultiert, wird, außer falls durch unmittelbare Verhandlung beigelegt, durch das Gericht der internationalen Handelsschiedsgerichtsbarkeit bei der Industrie- und Handelskammer der Russischen Föderation in Moskau, in der Russischen Föderation, beigelegt. Jeder vom Schlichter abgegebene Schiedsspruch ist für die beteiligten Parteien endgültig und bindend und jedwedes Urteil bezüglich eines solchen Schiedsspruchs kann von jedem Gericht der zuständigen Jurisdiktion durchgesetzt werden. Nichts in diesem Abschnitt 11 wird eine Partei daran hindern, von einem Gericht der zuständigen Jurisdiktion rechtmäßige Entschädigung zu verlangen oder zu erhalten, sei es vor, während oder nach einem Schiedsverfahren.

11. Zeitraum für Rechtsverfolgung.

Von den Parteien dieses Vertrags kann keine Rechtsverfolgung, ungeachtet der Form, die sich aus Transaktionen unter diesem Vertrag ergibt, nach mehr als einem (1) Jahr nach dem Eintreten des Klagegrundes oder der Entdeckung dessen Eintritts ergriffen werden, außer, dass eine Rechtsverfolgung für Verletzung von Rechten geistigen Eigentums innerhalb des maximal geltenden gesetzlichen Zeitraums ergriffen wird.

12. Vollständigkeit der Vereinbarung, Salvatorische Klausel, kein Verzicht.

Dieser Vertrag stellt die Gesamtvereinbarung zwischen Ihnen und dem Rechtsinhaber dar und ersetzt jegliche sonstigen, vorherigen Vereinbarungen, Vorschläge, Kommunikation oder Ankündigung, ob mündlich oder schriftlich, in Bezug auf die Software oder den Gegenstand dieser Vereinbarung. Sie bestätigen, dass Sie diesen Vertrag gelesen haben, ihn verstehen und seinen Bedingungen zustimmen. Falls eine Bestimmung dieses Vertrags von einem Gericht der zuständigen Jurisdiktion insgesamt oder in Teilen als untauglich, ungültig oder aus welchen Gründen auch immer als nicht durchsetzbar angesehen wird, wird diese Bestimmung enger ausgelegt, damit sie rechtmäßig und durchsetzbar wird, und der Gesamtvertrag wird an diesem Umstand nicht scheitern, und die Ausgewogenheit des Vertrags bleibt weiterhin vollinhaltlich gültig und wirksam, so weit gesetzlich oder nach Billigkeitsrecht zulässig, während der ursprüngliche Inhalt weitest möglich beibehalten wird. Kein Verzicht auf eine hierin enthaltene Bestimmung oder Kondition ist gültig, außer in schriftlicher Form und durch Sie und einen autorisierten Vertreter des Rechtsinhabers unterzeichnet, vorausgesetzt, dass kein Verzicht einer Verletzung einer Bestimmung dieses Vertrags einen Verzicht eines vorherigen, gleichzeitigen oder Folgeverstoßes konstituiert. Nichtverfolgung oder fehlende Durchsetzung einer Bestimmung dieses Vertrags durch den Rechtsinhaber kann nicht als Verzicht auf diese Bestimmung oder dieses Recht geltend gemacht werden.

14. Ansprechpartner des Rechtsinhabers

Sollten Sie Fragen in Bezug auf diesen Vertrag haben oder sollten Sie wünschen, sich aus irgendeinem Grund mit dem Rechtsinhaber in Verbindung zu setzen, kontaktieren Sie bitte unsere Kundendienstabteilung unter:

Kaspersky Lab ZAO, 10 build. 1, 1st Volokolamsky Proezd
Moskau, 123060
Russische Föderation
Tel.: +7-495-797-8700
Fax: +7-495-645-7939
E-Mail: info@kaspersky.com
Webseite: www.kaspersky.com

KASPERSKY LAB

Kaspersky Lab wurde 1997 gegründet. Die Firma ist heute das bekannteste Unternehmen für Datenschutz-Software in Russland und bietet eine breite Palette an IT-Sicherheitslösungen zum Schutz vor Viren, Spam und Hackerangriffen.

Kaspersky Lab ist ein international operierender Konzern. Der Stammsitz befindet sich in Russland. Das Unternehmen unterhält Niederlassungen in Großbritannien, Frankreich, Deutschland, Japan, in den Beneluxstaaten, in China, Polen, Rumänien und in den USA. In Frankreich wurde eine neue Filiale gegründet, das Europäische Zentrum für Antivirenforschung. Unser Partnernetzwerk verbindet weltweit mehr als 500 Unternehmen.

Kaspersky Lab – das ist heute mehr als tausend hoch qualifizierte Fachleute, von denen ein Dutzend MBA-Diplome, sechzehn einen Doktortitel haben. Die führenden Virusanalytiker von Kaspersky Lab gehören zur prestigeträchtigen Computer Anti-virus Researcher's Organization (CARO).

Das größte Kapital des Unternehmens besteht in dem einzigartigen Wissen und in der Erfahrung, die von den Mitarbeitern im Laufe des mehr als vierzehnjährigen kontinuierlichen Kampfes gegen Viren gesammelt wurden. Dank der permanenten Analyse von Virenaktivitäten sind wir in der Lage, Tendenzen in der Malware-Entwicklung zu prognostizieren und unseren Benutzern rechtzeitig zuverlässigen Schutz vor neuen Angriffen zu gewährleisten. Dieser Vorteil manifestiert sich in den Erzeugnissen und Leistungen von Kaspersky Lab. Wir sind unseren Konkurrenten stets einen Schritt voraus und bieten unseren Kunden Schutz von höchster Güte.

Aufgrund der jahrelangen Tätigkeit ist das Unternehmen jetzt ein führender Entwickler im Bereich der Virenschutztechnologien. Kaspersky Lab hat als erstes Unternehmen viele moderne Standards für Antiviren-Software gesetzt. Die Basisprodukt des Unternehmens heißt Kaspersky Anti-Virus®. Es bietet für alle Arten von Objekten zuverlässigen Schutz vor Virenangriffen: Arbeitsstationen, Dateiserver, Mailsysteme, Firewalls und Internet-Gateways, Handhelds. Bequeme Steuerelemente erlauben es dem Benutzer, den Antivirenschutz von Computern und Firmennetzwerken möglichst weitgehend zu automatisieren. Viele von Welt-Entwicklern verwenden in ihrer Software den Kern vom Kaspersky Anti-Virus®. Zu ihnen gehören u.a.: Nokia ICG (USA), Aladdin (Israel), Sybari (USA), G Data (Deutschland), Deerfield (USA), Alt-N (USA), Microworld (Indien), BorderWare (Kanada).

Die Kunden von Kaspersky Lab kommen in den Genuss eines breiten Spektrums von Zusatzleistungen, die das störungsfreie Funktionieren der Erzeugnisse und die genaue Kompatibilität mit speziellen Business-Vorgaben garantieren. Wir planen, realisieren und begleiten komplexe Antivirenlösungen für Unternehmen. Unsere Datenbanken werden stündlich aktualisiert. Rund um die Uhr steht unseren Benutzern ein technischer Kundendienst in mehreren Sprachen zur Verfügung.

Sollten Sie weitere Informationen wünschen, wenden Sie sich bitte an unsere Vertriebspartner oder direkt an Kaspersky Lab. Wir werden Sie gerne telefonisch oder per E-Mail beraten. Alle Ihre Fragen werden umfassend beantwortet.

Webseite von Kaspersky Lab:	http://www.kaspersky.com/de/
Viren-Enzyklopädie:	http://www.viruslist.com/de/
Kontakt:	http://www.kaspersky.de/kontakt
Technischer Support:	http://support.kaspersky.de
Feedback zu unseren Benutzerhandbüchern:	
Antiviren-Labor:	newvirus@kaspersky.com (nur zum Einsenden verdächtiger Objekte, die zuvor archiviert wurden) http://support.kaspersky.ru/virlab/helpdesk.html?LANG=de (für Fragen an die Virenanalytiker)
Webforum von Kaspersky Lab:	http://forum.kaspersky.com

SACHREGISTER

Q

R

S

U

V

W